625-CD-517-002

EOSDIS Core System Project

ECS Training Material
Volume 17: System Troubleshooting

April 2000

Raytheon Systems Company
Upper Marlboro, Maryland

ECS Project Training Material
Volume 17: System Troubleshooting

April 2000

Prepared Under Contract NAS5-60000
CDRL Item 129

RESPONSIBLE ENGINEER

Paul E. Van Hemel /s/ 4/6/00

Paul E. Van Hemel Date
EOSDIS Core System Project

SUBMITTED BY

Gary Sloan /s/ 4/6/00

Gary Sloan, M&O Manager Date
EOSDIS Core System Project

Raytheon Systems Company
Upper Marlboro, Maryland

625-CD-517-002

This page intentionally left blank.

Preface

This document is a contract deliverable with an approval code of 3. As such, it does not require formal Government approval. This document is delivered for information only, but is subject to approval as meeting contractual requirements.

Any questions should be addressed to:

Data Management Office
The ECS Project Office
Raytheon Systems Company
1616 McCormick Dr.
Upper Marlboro, MD 20774-5301

This page intentionally left blank.

Abstract

This is Volume 17 of a series of lessons containing the training material for Release 5B of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS). This lesson provides a detailed description of the different tasks that are required to perform system troubleshooting. The lesson includes a detailed review of the system monitoring capabilities, hardware and software troubleshooting process, and trouble ticket set-up and processing.

Keywords: training, instructional design, course objective, system troubleshooting, trouble ticket, HP OpenView, maintenance, Inventory/Logistical Management (ILM) tool

This page intentionally left blank.

Change Information Page

List of Effective Pages	
Page Number	**Issue**
Title	Revised
iii through xii	Revised
1 through 142	Revised
Slide Presentation 1 through 97	Revised

Document History			
Document Number	**Status/Issue**	**Publication Date**	**CCR Number**
625-CD-517-001	Original	July 1999	
625-CD-517-002	Revised	April 2000	

This page intentionally left blank.

Contents

Configuration Parameters

System Performance Monitoring

Problem Analysis/Troubleshooting

Troubleshooting of Custom Software

Trouble Ticket (TT)

Practical Exercise

Slide Presentation

Introduction

Identification

Training Material Volume 17 is part of Contract Data Requirements List (CDRL) Item 129, whose requirements are specified in Data Item Description (DID) 625/OP3 and is a required deliverable under the Earth Observing System Data and Information System (EOSDIS) Core System (ECS), Contract (NAS5-6000).

Scope

Training Material Volume 17 describes the process and procedures for ECS System Troubleshooting. This lesson is designed to provide the operations staff with sufficient knowledge and information to satisfy all lesson objectives.

Purpose

The purpose of this Student Guide is to provide a detailed course of instruction that forms the basis for understanding System Troubleshooting. Lesson objectives are developed and will be used to guide the flow of instruction for this lesson. The lesson objectives will serve as the basis for verifying that all lesson topics are contained within this Student Guide and slide presentation material.

Status and Schedule

This lesson module provides detailed information about training for Release 5B. Subsequent revisions will be submitted as needed.

Organization

This document is organized as follows:

Introduction:	The Introduction presents the document identification, scope, purpose, and organization.
Related Documentation:	Related Documentation identifies parent, applicable and information documents associated with this document.
Student Guide:	The Student Guide identifies the core elements of this lesson. All Lesson Objectives and associated topics are included.
Slide Presentation:	Slide Presentation is reserved for all slides used by the instructor during the presentation of this lesson.

This page intentionally left blank.

Related Documentation

Parent Document

The parent document is the document from which this ECS Training Material's scope and content are derived.

423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work

Applicable Documents

The following documents are referenced within this ECS Training Material, or are directly applicable, or contain policies or other directive matters that are binding upon the content of this document:

420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-02	Goddard Space Flight Center, Functional and Performance Requirements Specification for the Earth Observing System Data and Information System (EOSDIS) Core System (ECS)

Information Documents

Information Documents Referenced

The following documents are referenced herein and amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS Training Material.

609-CD-510	Release 5B Operations Tools Manual for the ECS Project
611-CD-510	Mission Operation Procedures for the ECS Project

Information Documents Not Referenced

The following documents, although not referenced herein and/or not directly applicable, do amplify or clarify the information presented in this document. These documents are not binding on the content of the ECS Training Material.

305-CD-510	Release 5B Segment/Design Specification for the ECS Project
311-CD-520	Release 5B Data Management Subsystem Database Design and Database Schema Specifications for the ECS Project
311-CD-521	Release 5B INGEST Database Design and Database Schema Specifications for the ECS Project

311-CD-522	Release 5B Interoperability Subsystem (IOS) Database Design and Database Schema Specifications for the ECS Project
311-CD-523	Release 5B Planning and Data Processing Subsystem Database Design and Schema Specifications for the ECS Project
311-CD-524	Release 5B Science Data Server Database Design and Schema Specifications for the ECS Project
311-CD-525	Release 5B Storage Management and Data Distribution Subsystems Database Design and Database Schema Specifications for the ECS Project
311-CD-526	Release 5B Subscription Server Database Design and Schema Specifications for the ECS Project
311-CD-527	Release 5B Systems Management Subsystem Database Design and Schema Specifications for the ECS Project
311-CD-528	Release 5B Registry Database Design and Schema Specifications for the ECS Project
313-CD-510	Release 5B ECS Internal Interface Control Document for the ECS Project
334-CD-510	5B Science System Release Plan for the ECS Project
601-CD-001	Maintenance and Operations Management Plan for the ECS Project
603-CD-003	ECS Operational Readiness Plan for Release 2.0
604-CD-001	Operations Concept for the ECS Project: Part 1-- ECS Overview
604-CD-002	Operations Concept for the ECS Project: Part 2B -- ECS Release B
605-CD-002	Release B SDPS/CSMS Operations Scenarios for the ECS Project
607-CD-001	ECS Maintenance and Operations Position Descriptions
152-TP-001	ACRONYMS for the EOSDIS Core System (ECS) Project
152-TP-003	Glossary of Terms for the EOSDIS Core System (ECS) Project
211-TP-005	Transition Plan 4PX to 4PY, 4PY to 5A, and 5A to 5B for the ECS Project
220-TP-001	Operations Scenarios - ECS Release B.0 Impacts
500-1002	Goddard Space Flight Center, Network and Mission Operations Support (NMOS) Certification Program, 1/90
535-TIP-CPT-001	Goddard Space Flight Center, Mission Operations and Data Systems Directorate (MO&DSD) Technical Information Program Networks Technical Training Facility, Contractor-Provided Training Specification

System Troubleshooting Overview

Lesson Overview

This lesson will provide you with the process for system/performance monitoring, problem analysis and troubleshooting of system hardware and software, and administration of the trouble ticket system. It provides practical experience in using the tools you will need for resolving system problems and minimizing system down time.

Lesson Objectives

Overall Objective - The overall objective of this lesson is proficiency in the methodology and procedures for system troubleshooting of the Earth Observing System Data and Information System (EOSDIS) Core System (ECS).

Condition - The student will be given a copy of 611-CD-510-001 *Mission Operation Procedures for the ECS Project*, 609-CD-510-002 *Release 5B Operations Tools Manual*, and a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the tools in accordance with prescribed methods and complete required procedures without error.

Specific Objective 1 - The student will conduct system performance monitoring, to include checking the health and status of the network and accessing the EOSDIS Backbone Network (EBnet) Web Page.

Condition - The student will be given a copy of 611-CD-510-001 *Mission Operation Procedures for the ECS Project*, 609-CD-510-002 *Release 5B Operations Tools Manual*, and a workstation console with access to HP OpenView.

Standard - The student will use HP OpenView in accordance with specified procedures and without error to examine maps for color alerts and new nodes, create special submaps for monitoring status, and check for event notifications.

Specific Objective 2 - The student will perform problem analysis and troubleshooting, to include analysis and troubleshooting of the system, analysis and troubleshooting of commercial off-the-shelf (COTS) hardware and software.

Condition - The student will be given a copy of 611-CD-510-001 *Mission Operation Procedures for the ECS Project*, 609-CD-510-002 *Release 5B Operations Tools Manual*, and a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the GUI tools without error in accordance with applicable procedures to perform the required troubleshooting and maintenance activities.

Specific Objective 3 - The student will use the Inventory/Logistical Management (ILM) tool to prepare a maintenance work order and a maintenance work order modification.

Condition - The student will be given a copy of 611-CD-510-001 *Mission Operation Procedures for the ECS Project*, 609-CD-510-002 *Release 5B Operations Tools Manual*, and a workstation console with access to ECS software tools including the ILM tool.

Standard - The student will use the ILM tool without error in accordance with applicable procedures to prepare the required work order and work order modification.

Specific Objective 4 - The student will perform the procedures required for switchover from a failed primary processor to a backup processor and switch back to the primary processor upon its return to service.

Condition - The student will be given a copy of 611-CD-510-001 *Mission Operation Procedures for the ECS Project* and workstation consoles with access to ECS software tools.

Standard - The student will perform the necessary procedures without error and complete the initial switchover in less than 30 minutes.

Specific Objective 5 - The student will perform the procedures required for general check out and diagnosis of failures related to operations with custom ECS software.

Condition - The student will be given troubleshooting procedures, a copy of 611-CD-510-001 *Mission Operation Procedures for the ECS Project*, 609-CD-510-002 *Release 5B Operations Tools Manual*, and a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard -The student will use the information and available tools without error in accordance with applicable procedures to perform the required troubleshooting activities.

Specific Objective 6 - The student will perform the functions required to set up and manage trouble ticket processing, including administrative set-up of user accounts and privileges in the trouble ticket software.

Condition - The student will be given a copy of 611-CD-510-001 *Mission Operation Procedures for the ECS Project*, 609-CD-510-002 *Release 5B Operations Tools Manual*, and a workstation console with access to ECS software tools including Trouble Ticket, Fault/Performance Management, HP OpenView, and Management Services Subsystem (MSS) graphical user interface (GUI) tools.

Standard - The student will use the GUI tools without error in accordance with applicable procedures to perform the required trouble ticket functions.

Importance

This lesson provides students with the knowledge and skills needed for effective system troubleshooting and maintenance of the ECS. It is structured to provide useful skills and knowledge concerning ECS operation and the tools for identifying system problems and returning malfunctioning system hardware and software to normal operational status. It provides useful instruction and practical exercises in maintaining ECS in an operationally ready condition, and is therefore vital to students who are preparing for a number of different positions with responsibilities in maintaining that system readiness, including positions as:

- Computer Operator, System Administrator, and Maintenance Coordinator at the DAAC.
- System Engineer, System Test Engineer, System Administrator, and Software Maintenance Engineer at the System Operational Support (SOS) group or at the Sustaining Engineering Organization (SEO).
- System Engineer, System Test Engineer, and Software Maintenance Engineer at the DAAC.

This page intentionally left blank.

Configuration Parameters€

There are many configurable parameters associated with ECS software. Some of them are set by default to values that may be appropriate for most operating conditions. Others may be set to values that may or may not be appropriate for the requirements of operations at a particular DAAC. Some parameters may be changed using ECS Graphical User Interfaces (GUIs) specifically designed to monitor and control functions related to particular subsystems. Others may require changes to a configuration file (i.e., edit the file using UNIX vi editor) or database (typically done by the Database Administrator). ***Note: Before changing any configuration parameter, make certain either that it is not under configuration control or that you have obtained any necessary approval specified in local Configuration Management policies and procedures.***

Configuration Registry

As of the second delivery for Software Release 5B, ECS configuration parameters are manageable by a *Configuration Registry*. The Configuration Registry Server provides a single interface to retrieve configuration attribute-value pairs for ECS Servers from the Configuration Registry Database, via a Sybase Server. The Configuration Registry Server maintains an internal representation of the tree in which configuration attribute-value pairs are stored. General configuration parameters used by many servers are stored in higher nodes in the tree. Parameters specific to a single ECS Server are contained in the leaf nodes of the tree. ECS provides a script tool to load the Configuration Registry database from data in configuration files. Once the Configuration Registry is loaded, if the configuration files are moved or otherwise made inaccessible to the software, the software goes to the Configuration Registry to obtain needed configuration parameters. There is also a Configuration Registry GUI to view and edit configuration data in the database. Changes to the Configuration Registry typically are under the control of the Database Administrator and Configuration Management.

General Configuration Parameters

Training lessons for specific DAAC functions (e.g., Ingest, Production Planning and Processing, Data Distribution) address configuration parameters related to those functions. Table 1 identifies some of the more generically applicable ECS subsystem configuration files, key system parameters, known defaults, and known desirable values along with known effects or factors that may influence the values to which they are set. This is a very limited and preliminary representation of a large amount of configuration parameter information that ECS is making available in published and dynamic baseline information. More information, including data on parameters, units of measure, defaults, recommendations, and site/platform specific UNIX parameters can be obtained on the web at http://cmdm.east.hitc.com, in the 920 series of Technical Documents.

Table 1. General Configuration Parameters

File(s)	Parameter	Default Value	Desired Value and Known Effects/Factors
Various (one for each application, e.g., EcDsScienceDataServer.CFG)	ApplLogSize	= 50000 to = 1000000	Varied; For Ingest, = 50000 For DPS, = 200000 For SDSRV, = 5000000 For DDIST, = 1000000
	AppLogLevel	0	Discretionary; 0 provides a full trace recording of all events, 1 provides messages related to all major events, 2 yields just records of errors, and 3 turns recording off.
	DebugLevel	3	Discretionary; 3 provides a full trace recording of all events, 2 provides messages related to all major events, 1 yields just records of errors, and 0 turns recording off. The Debug level for SDSRV and the HDF EOS Server should be set to 2. Level 2 will display messages when SDSRV is making a RPC to another server or SYBASE. When the Debug level is set to three, large amounts of metadata are output to the log file. For searches of granules that have big descriptors (Landsat), the difference in the search time can be as much as 30 times more if the debug level is set to 3.

Table 1. General Configuration Parameters (continued)

File(s)	Parameter	Default Value	Desired Value and Known Effects/Factors
EcDsScienceDataServer.CFG	DSS_NUM_GEN_CATALOGS	15	Controls how many DsMdCatalog objects get created within SDSRV on startup; has direct impact on the number of SYBASE connections held by SDSRV.
	SDSRV_CATALOG_CONNECT_INSTRUCTIONS	SQSOnly	Controls how the DsMdCatalog connects to the database; default causes each object to create only 1 connection. Setting the value to "SybaseAndSQS" causes each object to create two connections and offers performance gains by using direct SQL Server connections where possible. Do not set to "SybaseOnly" because it will then not support spatial data processing.
	SDSRV_AUTO_INSPECT_SWITCH	On	Controls whether SDSRV returns commonly inspected metadata attributes as part of search requests; when the value is "on" a Remote Procedure Call (RPC) is eliminated for frequently inspected attributes.
	SDSRV_NUM_INT_SESSION	128	Controls the maximum number of concurrent sessions SDSRV will start to execute asynchron-ous acquire requests in the queue. If this number is set too low and there are a lot of Landsat requests, the other requests may never be serviced.
	NumOfHDFServer	3	(*NOTE*: HDF-EOS Servers required only at sites doing Landsat-7 distribution.) Should be a minimum of 3.

Table 1. General Configuration Parameters (continued)

File(s)	Parameter	Default Value	Desired Value and Known Effects/Factors
EcDsStArchiveServer.CFG	CHECKSUMSTATUS	OFF	Controls whether a checksum is calculated for each file inserted into the archive. If value is ON, this time-consuming and CPU-intensive process can have a significant impact on performance.
	ListenThreads	7	Maximum = 125
EcDsStStagingMonitorServer.CFG	CHECKSUMSTATUS	OFF	Controls whether a checksum is calculated for each file acquired from the archive. If value is ON, this time-consuming and CPU-intensive process can have a significant impact on performance.
	ListenThreads	7	Maximum = 125
EcDsStPullMonitorServer.CFG	ListenThreads	1	Pull Monitor is single threaded
EcDsStStagingDiskServer.CFG	ListenThreads	7	Maximum = 125
EcDsStFtpDisServer.CFG	ListenThreads	7	Based on DCE practice of setting the inbound rpc queue to no more than 8 times the number of Pull Monitor listen threads; if there are more than 8 FtpDis listen threads, some of the requests sent to Pull Monitor may be lost.
EcDsStIngestFtpServer.CFG	ListenThreads	7	Maximum = 125
EcDsStD3Server.CFG	ListenThreads	7	Only one request can be processed at a time.
EcDsSt8MMServer.CFG	ListenThreads	2	Threads for each request from DDIST for media distribution, plus extra for pinging the server; value can be up to 30.

Table 1. General Configuration Parameters (continued)

File(s)	Parameter	Default Value	Desired Value and Known Effects/Factors
EcDsStPrintServer.CFG	ListenThreads	7	Number of physical media devices being used up to a maximum of 125; realistically, 1 would be sufficient in most cases because there are no long-running processes done by the print server
EcMsAgSubAgent.ACFG	MsAg_LogMaxSize	1000000	190000
	MsAg_LogLevel	1	1
	MsAg_MssEventLevel	1	1
	MsAg_LocalPollInterval_sec	15	15
	MsAg_MetricRefreshInterval_sec	2	2
	MsAg_DiscoverInterval_sec	1200	1200
	MsAg_RetrySleep_sec	30	30
	MsAg_NumRetries	10	10
EcMsAgSubAgent.PCFG	MsAg_UpdateInterval_sec	99	99
	MsAg_AppShutdown_sec	20	20
	MsAg_ProgShutdown_sec	15	15
	MsAg_ProcShutdown_sec	10	10
EcMsAgSubAgent.CFG	DebugLevel	3	3

Table 1. General Configuration Parameters (continued)

File(s)	Parameter	Default Value	Desired Value and Known Effects/Factors
EcMsDeputyAgent.ACFG	MsAg_LogMaxSize	10000	10000
	MsAg_LogLevel	0	0
	MsAg_RetrySleep-sec	172800	172800
EcMsDeputyAgent.PCFG	MsAg_UpdateInterval_sec	99	99
	MsAg_AppShutdown_sec	20	20
	MsAg_ProgShutdown_sec	15	15
	MsAg_ProcShutdown_sec	10	10
EcMsDeputyAgent.CFG	DebugLevel	0	3

Although Table 1 addresses many important configuration parameters, it does not provide an exhaustive list, even of general configuration parameters. The values assigned to system parameters can affect ECS functioning and performance. Any changes that are considered need to be investigated in view of anticipated changes in the way the system operates. When troubleshooting system problems, it may also be helpful to determine whether there have been any recent changes to system parameters that could be responsible for impaired performance, and to reset suspect parameters to default and/or recommended values, coordinating with the Database Administrator or Configuration Management Administrator as appropriate.

System Performance Monitoring€

The key to maintaining ECS in an operationally ready state is effective performance monitoring.

- System operators – close monitoring of progress and status of system and subsystem functions that are the focus of their jobs.
  - Notice any serious degradation of system performance that has an impact on their abilities to conduct their jobs successfully and meet user needs.
- System administrators and system maintenance personnel – monitor overall system functions and performance.
  - Administrative and maintenance oversight of system.
  - Watch for system problem alerts.
  - Use monitoring tools to create special monitoring capabilities.
  - Check for notification of system events.

Log in to ECS

Many system monitoring and troubleshooting procedures require logging in to ECS, and may involve remote access to distributed hosts. When log in is required in the many procedures specified in this lesson, the procedure simply states "Log in to the host for . . ." or "At the UNIX prompt on the host for . . ." to avoid needless repetition of steps that are likely to be well known. The log-in steps, using the secure shell (ssh) protocol, are presented once here for reference. These steps assume that the operator is logged completely out of the system at the beginning. To log in, use the following procedure.

Log in to ECS

1 To access the desktop environment, enter your user ID and password at the initial screen.

- The Common Desktop Environment (CDE) is displayed.

2 To access a UNIX terminal window, select "Terminal" from the pull-up menu at the arrow button at the bottom of the window.

- The Common Desktop Environment (CDE) is displayed.

3 If you will want to display a Graphical User Interface (GUI) at the local terminal, it may be necessary to type **setenv DISPLAY <*local terminal ID (e.g., ip address*>:0.0** and then press the **Return/Enter** key.

- The **DISPLAY** variable may default to the desired terminal; to check it, type **echo $DISPLAY**, and then press the **Return/Enter** key.
  - The set value of the **DISPLAY** variable is displayed.

4 To start the log-in to the desired remote host, type **/tools/bin/ssh <*hostname*>** and then press the **Return/Enter** key.

- If you receive the message, **Host key not found from the list of known hosts. Are you sure you want to continue connecting (yes/no)?** type **yes** ("**y**" alone does not work).
- If you have previously set up a secure shell passphrase and executed **sshremote**, a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears; continue with Step 5.
- If you have not previously set up a secure shell passphrase; go to Step 6.
- ***Note***: If you need to log in to the remote host as an account other than yourself (e.g., **root**), the ssh command takes the form **ssh -l <*account*> <*hostname*>**.

5 If a prompt to **Enter passphrase for RSA key '<*user@localhost*>'** appears, type your ***Passphrase*** and then press the **Return/Enter** key. Go to Step 7.

- The prompt indicates successful log in to the selected host.

6 At the **<*user@remotehost*>'s password:** prompt, type your ***Password*** and then press the **Return/Enter** key.

- The prompt indicates successful log in to the selected host.

7 Log in is complete.

Checking the Health and Status of the Network

ECS is heavily dependent on the use of computer networks. HP OpenView is a management tool that provides operators and maintainers with a system view for monitoring and checking the network, for quickly identifying parts of the network that may have problems, and for isolating faults on the network. It provides the following general features:

- a site-wide view of network and system resources.
- status information on resources.
- event notifications and background information.
- operator interface for starting servers and managing resources.

Specific monitoring capabilities provided by HP OpenView Network Node Manager (NNM) include:

- a network map showing elements and services with color alerts to indicate problems.
- indication of network and server status and changes.
- creation of submaps for special monitoring.

- event notifications.

Figure 1 shows an example of network map screens from HP OpenView.

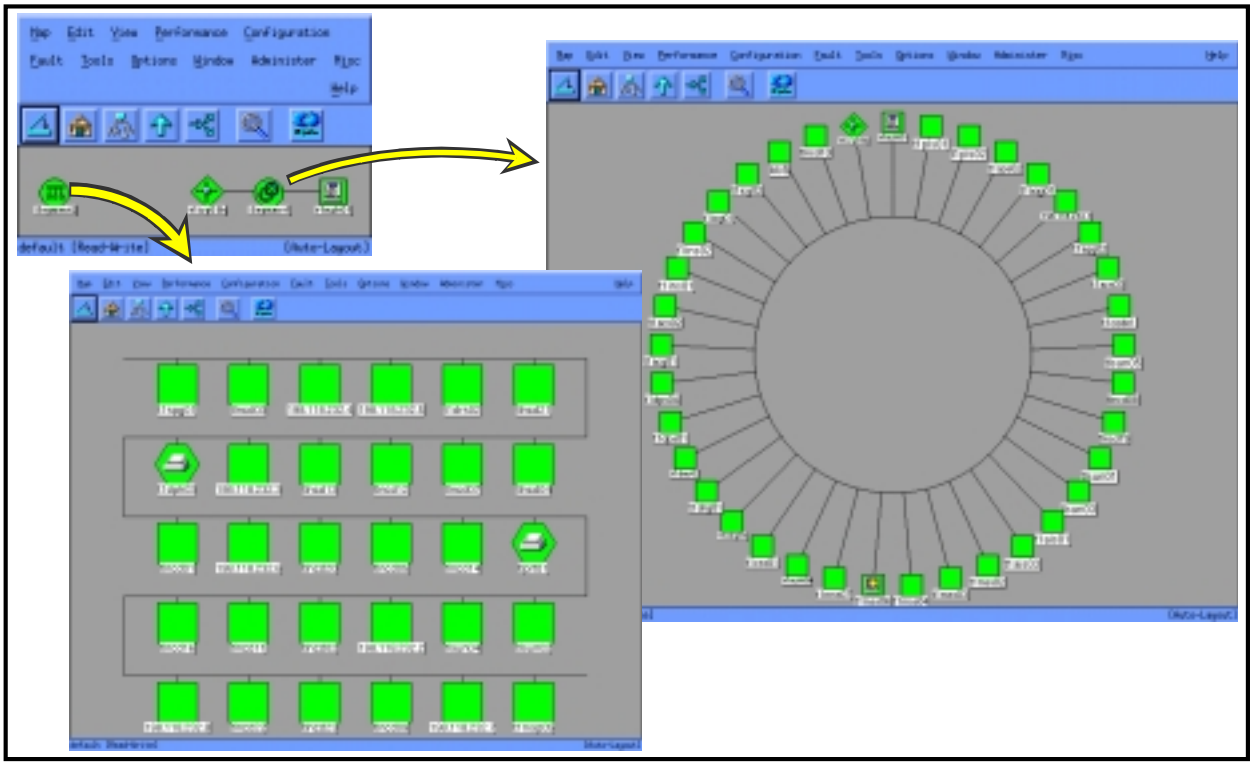


Figure 1. Example of Network Map Screens from HP OpenView

HP OpenView is capable of discovering a network and its elements. To use HP OpenView NNM to monitor the network, it must be running and configured to display status, with its Network map set for read-write and the Internet Protocol (IP) map enabled.

Starting and Ending a NNM Session

For NNM to report properly on the network topography, HP OpenView Windows (OVW) must be activated. Once activated, OVW automatically starts NNM, as well as any installed and registered NNM applications. As a prerequisite, the network management processes that work with OVW and NNM must be running. These network management processes are:

- **ovwdb** - the process that maintains the OVW database.
- **trapd** - the process that multiplexes and logs SNMP traps.
- **ovtopmd** - the process that maintains the network topology database.
- **ovactiond** - the process that executes commands upon receipt of an event.
- **snmpCollect** - the process that collects MIB data and performs threshold monitoring.

- **netmon** - the process that polls SNMP agents for initial discovery of the network topology and for detecting changes in the network topology, configuration, and status.

To see if these processes are running, type **/usr/ecs/*mode*/COTS/OV/bin/ovstatus** at a UNIX prompt on the HP OpenView server, where ***mode*** is likely to be **OPS**, **TS1**, or **TS2**.

To perform the start-up, use the following procedure.

Start the HP OpenView Windows NNM Graphical User Interface

1 On workstation ***x*0msh*##***, at the UNIX prompt in a terminal window, type **/usr/ecs/*mode*/COTS/OV/bin/ovstatus** (where ***mode*** is likely to be **OPS**, **TS1**, or **TS2**) and then press the **Return** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL; the ***##*** will be an identifying two-digit number (e.g., **l0msh03** indicates a management services subsystem *hp* workstation at LaRC).
- A series of messages is displayed indicating for each process that its state is "**RUNNING**" or "**NOT_RUNNING**."
- If the network management processes are not running, a system administrator (logged in as **root**) can start them by typing **/usr/ecs/*mode*/COTS/OV/bin/ovstart** (where ***mode*** is likely to be **OPS**, **TS1**, or **TS2**) and then pressing the **Return** key.

2 Type **/usr/ecs/*mode*/COTS/OV/bin/ovw &** and press the **Return** key.

- The **About OVW** box is displayed, followed in a few moments by the OVW submap window, and any installed and registered NNM applications are also started.
- The **Event Categories** window is displayed in the upper right corner of the screen.

To exit NNM and all other integrated applications, use the following procedure.

Exit NNM

1 From the menu bar on any submap window, follow menu path **Map→Exit**.

[or]

2 Click on the **Close** button on all open submap windows until the **Root** window is displayed. Then click on the **Close** button () on the **Root** window.

- The open map is saved and all submap windows and dialog boxes of the map are closed. OVW, all NNM applications, and all other integrated applications exit.

If you are logged in with HP OpenView NNM running you can get a quick assessment of the health and status of the network by checking the network map for color alerts. The symbols and the connections between them on the network map are color-coded to indicate status. There are two status categories:

- administrative – not propagated from child to parent through the network.
- operational – propagated from child to parent to indicate problems.

If the compound status (how status is propagated) for the open map is set to Default, the interpretation of the colors is as indicated in the table that appears in Figure 2. Note: If you have a color vision weakness, it is possible to change the colors displayed by HP OpenView. If you change them, make sure everyone who will use the software is aware of the changes.

Status Condition	Symbol Color	Connection Color
Unmanaged (a)	Off-white	Black
Testing (a)	Salmon	Salmon
Restricted (a)	Tan	Tan
Disabled (a)	Dark Brown	Dark Brown
Unknown (o)	Blue	Black
Normal (o)	Green	Green
Warning (o)	Cyan	Cyan
Minor/Marginal (o)	Yellow	Yellow
Major (o)	Orange	Orange
Critical (o)	Red	Red

(a) Administrative Status (o) Operational Status

Figure 2. HP OpenView Default Status Colors

Looking at maps for color alerts

To check your network for color alerts, you must first have the map for the network open. To open a map, use the following procedure:

Open a Network Map

1 With HP OpenView NNM running, follow menu path **Map→Open . . .**.

- The **Available Maps** dialog box is displayed.

2 Select the name of the map you want to open and click on "**Open Map**".

- A confirmation box is displayed.

3 Click on "**OK**".

- Any open map and its submap windows and dialogs close.
- The **Home Submap** (**Root**) of the selected map is displayed.

If you do not know the compound status scheme of the open map, follow the menu path **Map→Describe/Modify . . .** to obtain the **Map Description** dialog box and display/set the compound status scheme for default. Suppose there is a fault in an interface card in one of the workstations on your network. Use the following procedure to trace it using color alerts.

Looking at Maps for Color Alerts

1 Double click on the yellow **Internet** symbol.

- *Note*: The symbol will be yellow because the *critical* failure of the card in the workstation is propagated up to the level of the **Internet** symbol as a *minor* problem at that level.
- The **Internet submap** opens and displays the IP network(s). One IP network symbol is yellow. This indicates a marginal problem with the network.

2 Double click on the yellow **IP network** symbol.

- A **Network submap** opens and displays the segment(s) attached to the gateway(s). The segment symbol is yellow or cyan. This indicates a problem somewhere on the segment.

3 Double click on the yellow **segment** symbol.

- A **Segment submap** opens and displays the nodes attached to that segment. Of all the nodes in the segment, the workstation node is red. The problem is isolated to that workstation.

4 Double click on the red **workstation** symbol.

- A **Node submap** opens and displays its interface symbol. It is red.
- You have isolated the fault to a single card of a single node on your internet.

Looking at maps for new nodes

HP OpenView Windows includes an application called **IP Map** which, in default, is started automatically upon activation of HP OpenView Windows. IP Map creates network maps and submaps through several functions:

- automatically discovers all IP-addressable nodes on the network.
- creates an object for each discovered node.
- creates and displays symbols on the network map to represent created objects.
- creates a hierarchy of submaps to display the network in increasing detail.
  - internet submap.
  - network submaps.
  - segment submaps.
  - node submaps.

Each submap is assigned a layout algorithm that determines how its symbols are displayed. You can set automatic layout *on* or *off* to enable or disable enforcement of the layout algorithm, either for all submaps or for an individual submap. If autolayout is enabled, IP Map places new symbols directly on the submap. If autolayout is disabled, IP Map places new symbols in a **New Object Holding Area** in the lower part of the submap window. Symbols in the New Object Holding Area are shown without any connections. You can use HP OpenView to identify any new objects that are discovered and added to the open map. Suppose, for example, that a new workstation is added to the network and you wish to locate it and check its status. Use the following procedure to look for new nodes.

Looking at Maps for New Nodes

1 To check the default **Segment submap** for any new nodes that may have been discovered, open the default **Segment submap** from the segment symbol in the Network submap.

- View the submap for any new symbols.

2 To easily see new symbols in the submap, disable autolayout for the submap by following menu path **View→Automatic Layout→Off for this Submap**.

- When autolayout is disabled, a **New Object Holding Area** appears at the bottom of the submap.
- All newly added symbols are placed in the **New Object Holding Area**.

Creating special submaps for monitoring status

You can create submaps based on a logical organization rather than a physical one, to facilitate specialized monitoring. For example, suppose you want to have a submap just showing the Science Software Integration and Test (SSI&T) workstations at your site to have ready access to a display showing their status. Suppose further that you expect to use this submap frequently and therefore wish to create it within an existing hierarchy and be able to open it from a symbol in the Internet submap. Use the following procedure to create a special submap showing these workstations.

Creating Special Submaps for Monitoring Status

1 Decide where to locate your submap and whether it will have a parent or not.

- A submap without a parent object is independent of other existing submap hierarchies in the open map, and can be opened only from the **Available Submaps** dialog box. You can create child submaps of this submap, thereby creating a new submap hierarchy in the map.
- A submap that has a parent object can be opened from an explodable symbol of the parent object. If you want the new submap to exist within an existing submap hierarchy, you should create this submap from an explodable symbol.

2 To create a submap within an existing hierarchy, decide which symbol to use to open the new submap.

- If other symbols on the parent submap already open into child submaps or execute applications, you must create a new symbol to open the submap.

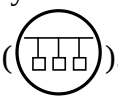
3 If you decide to create a new symbol (as in this case), add a symbol (for an existing object – in this case, a segment) or a new symbol and object to the submap of your choice (in this case, the Internet submap), by following menu path **Edit→Add Object . . . .**

- The **Add Object: Palette** window is displayed.

4 Click on the symbol representing the class of objects you want to add to the submap, using the scroll bar if necessary to scroll to the right for access to the desired symbol.

- For this training exercise, use the **Network Class**.
- The object symbols in the chosen class appear in the **Symbol Subclass** area of the **Add Object: Palette**.

5 Using the middle mouse button, drag the symbol representing the object to be added and drop it in the submap where it is to be added.

- You may add any of the symbols in the network class. For this training exercise, use the **bus** symbol ().
- The **Add Object** dialog box is displayed.

6 In the **Label Name** field of the **Add Object** dialog, type a label for the object (e.g., for this training exercise, type **SSI&T Workstations** and then click on the **OK** button.

- The entered label appears on the newly added blue symbol.

7 Open the new submap by double-clicking on the newly created symbol and then clicking on the **OK** button in the **Question** dialog that appears. Copy SSIS&T Workstation objects from other submaps into the newly created map, following menu path **Edit→Copy** and **Edit→Paste** operations.

- For more information about these operations, see the *HP OpenView Windows User's Guide*.

8 If desired, for each workstation copied, add its connection by following menu path **Edit→Add Connection . . . .**

- An **Add Connection** dialog is displayed, allowing you to select a type of connection (e.g., **Generic**), and then directing you to select a source and destination for the connection. You must then enter a selection name for the connection.
- When you click on **Close** for the **Add Connection** dialog, the newly added symbol changes color to indicate the status of its contained objects.

Checking for event notifications

Whenever a change occurs on the network, an **event** is generated. The occurrence of the event has two consequences:

- Through the internal processors of the **Network Node Manager**, the event is registered in a predefined category for display in an **Alarms Browser** window.
- The registration in the Events Browser window triggers a change for display in an **Alarm Categories** window (see Figure 3) to provide a notification that an event has occurred in the category of that Alarms Browser window. The display is a color change in a button on the Alarm Categories window corresponding to the event category. The color of the button indicates the highest severity event in the category. The default categories included in the Alarm Categories window are:
  - *Error Alarms*. This indicates inconsistent or unexpected behavior.
  - *Threshold Alarms*. This indicates that a threshold was exceeded.
  - *Status Alarms*. This indicates that an object or interface status changed to "up" or "down," or an object or interface started or stopped responding to Internet control message protocol (ICMP) echo requests.
  - *Configuration Alarms*. This indicates a node's configuration changed.
  - *Application Alert Alarms*. This indicates an HP OpenView Windows application generated an alarm or alert
  - *ECS Alarms (various)*: This indicates occurrence of an event in a category specifically defined for ECS.
  - *All Alarms*. This indicates one or more of the previously listed alarms occurred. Selecting this button lists all alarms in the listed categories and others in one dialog box.

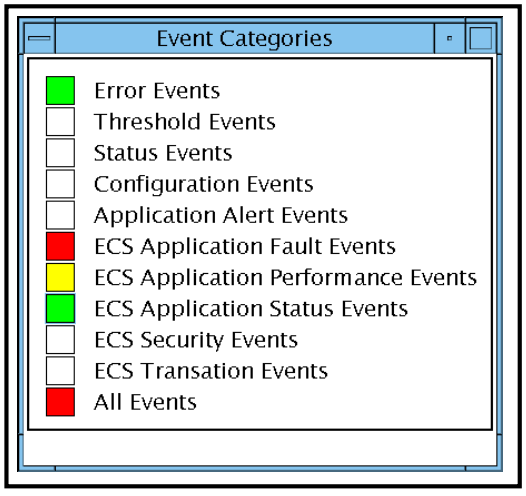


Figure 3. HP OpenView Alarm Categories Window

To check for event notifications, examine the Alarm Categories window to observe any color change in one or more of the buttons for the alarm categories. If there is a color change, you can click on the button to view its associated Alarms Browser window. For example, suppose you are monitoring the network when a critical threshold is exceeded somewhere on the network. Use the following procedure to check for event notifications.

Checking for Event Notifications

1 Observe that the **Threshold Alarms** button in the **Alarm Categories** window is red.

- This indicates that a critical threshold was exceeded somewhere on the network.

2 Click on the **Threshold Alarms** button in the **Alarm Categories** window. The **Threshold Alarms Browser** dialog box appears with a chronological listing of the threshold alarms that have occurred, with the most recent alarms at the bottom of the list.

- Each alarm listed includes the severity, time the alarm occurred, node on which the alarm occurred, and a brief alarm message.

3 To view the node that generated the alarm shown in this example, select the alarm from the list and click on **Action→Highlight Source on Map**.

- A map appears with the **busynode** node highlighted. At this point, select the highlighted node by clicking on it, and invoke appropriate operations from the menu bar to further diagnose and correct the situation that caused the threshold to be exceeded.

4 To delete the alarm, select the alarm and click on **Action→Delete→Selected Alarms**.

- This deletes only the selected alarm. (Note: multiple alarms may be selected and deleted.)

- For more information about alarm notification, click on the **help** button in the dialog box for the alarm being viewed or from the **Help: Index**, select **Show Entries with: alarm** (i.e., type **alarm** and click on the **Start Search** button).

Accessing the EOSDIS Backbone Network (EBnet) Web Page

The EBnet is a Wide Area Network (WAN) that provides, in combination with other institutional and public networks, connectivity between geographically distributed EOSDIS facilities to support ECS mission operations and data production functions. Specifically, its functions include:

- provides connectivity between the ECS DAACs, the EOS Data and Operations System (EDOS) facilities, affiliated data centers, and other designated EOSDIS sites.
- serves as the interface between EDOS, the DAACs, and the NASA Internet (NI).
- transporting spacecraft command, control, and science data nationwide on a continuous basis, 24 hours a day, 7 days a week.

- transports real-time mission-critical data related to the health and safety of on-orbit space systems and raw science telemetry as well as pre-launch testing and launch support.
- transports science data collected from spacecraft instruments and various levels of processed science data including expedited data sets, production data sets, and rate-buffered science data.
- provides wide-area communications through common carrier circuits for internal EOSDIS communications.
- interface to Exchange Local Area Networks (LANs) which provide communications between the WAN and site-specific LANs.

The NASA Communications (Nascom) organization at Goddard Space Flight Center (GSFC) maintains a home page for the EBnet (see Figure 4) on the World Wide Web at the following Universal Resource Location (URL):

- http://bernoulli.gsfc.nasa.gov/EBnet/.

This web site provides an overview of the EBnet as well as current data on its status and performance. Consequently, it can be a useful source of information when you are monitoring system performance. To access the EBnet Web Page, use the following procedure.

Accessing the EOSDIS Backbone Network (EBnet) Web Page

1 On workstation ***x*0msh##**, at the UNIX prompt in a terminal window, type **Netscape** at a UNIX command prompt and then press the **Return/Enter** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL; the **##** will be an identifying two-digit number (e.g., **l0msh03** indicates a management services subsystem *hp* workstation at LaRC).
- The starting page selected to appear on launch of the browser is displayed.

2 Click on the **Location** window of the starting page.

- The contents of the **Location** window are highlighted.

3 Enter **http://bernoulli.gsfc.nasa.gov/EBnet/** in the **Location** window.

4 Press the **Return/Enter** key on the keyboard.

- The EOSDIS Backbone Network (EBnet) home page is displayed.

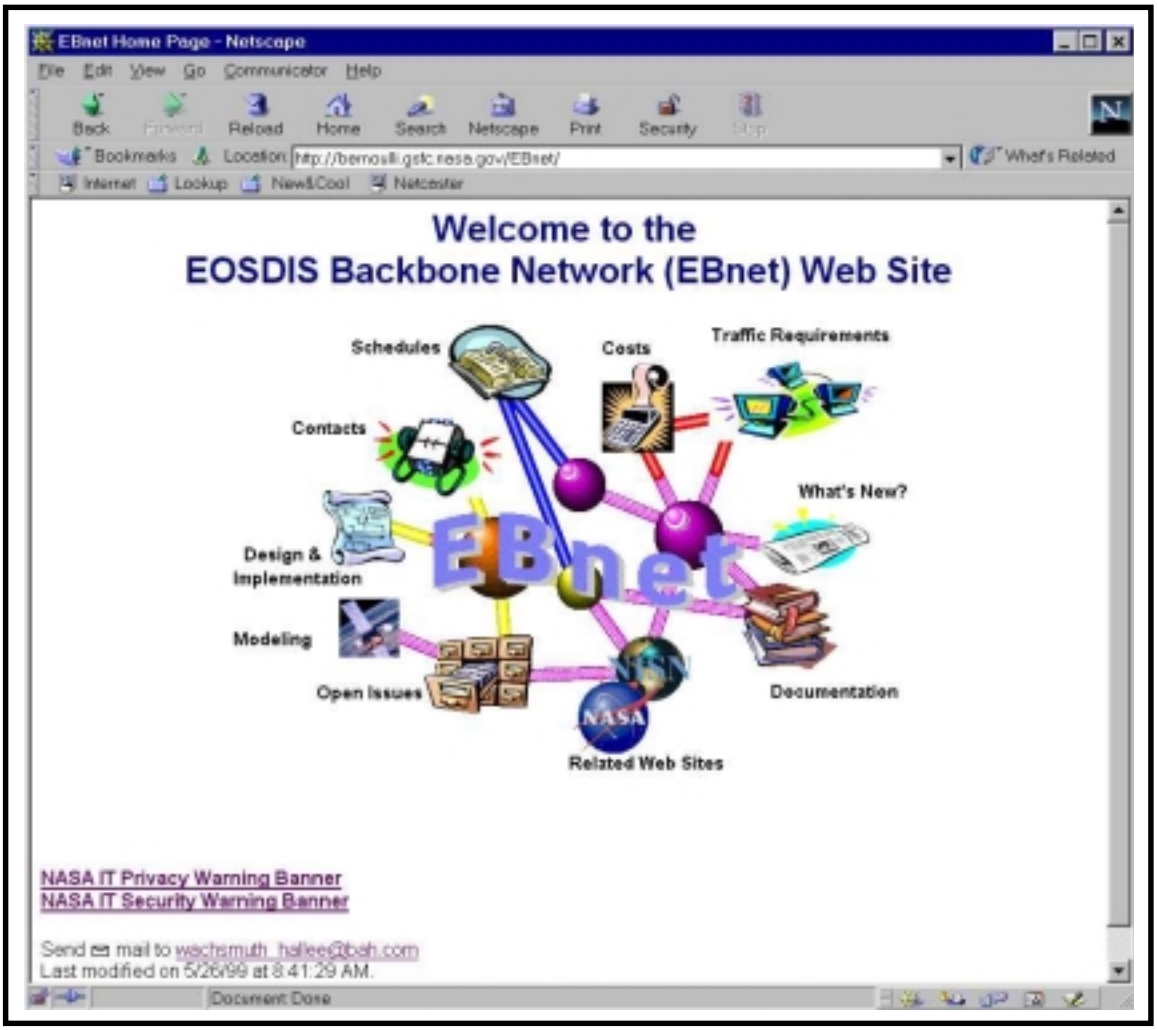


Figure 4. EBnet Home Page

This page intentionally left blank.

Problem Analysis/Troubleshooting

Although ECS is designed to be a robust computer network system, the complexity of its hardware and software components and interfaces provides a wealth of potential sources for system failures or other non-conformance problems. Fortunately, the tools available in ECS provide several avenues of assistance to help you detect and isolate problems in the system. Furthermore, there is an accumulating information base at the web site for the System Monitoring and Coordination Center (SMC) that may provide helpful insights and tips in solving system problems. The URL for the SMC site is **http://m0mss01.ecs.nasa.gov/smc/**. At the site, click on the link for Frequently Asked Questions (FAQ).

Analysis/Troubleshooting: System

Some of the Commercial Off-The Shelf (COTS) software products that are part of ECS provide alerts or warnings when there are system problems. For example,:

- HP OpenView.
  - color alerts to indicate problems.
- AutoSys/Xpert.
  - color/auditory alerts to indicate job status/failures.
- Tivoli.
  - "thermometer" icon showing high temperature to indicate failure.

Many of the COTS products as well as the software developed specifically for ECS generate error messages and event messages to indicate errors and status. The interpretation of these messages and suggested corrective actions can be found in 609-CD-510-002 *Release 5B Operations Tools Manual*. Several products also generate logs to capture and provide more detailed information about indicated problems. For example:

- HP OpenView.
  - event notifications/events browser; focus on all system events.
- Tivoli.
  - Tivoli Enterprise Console (TEC) system monitoring log; focus on software events.

As is ever the case with a complex system, the effectiveness of troubleshooting depends on knowledge of the system and its documentation, applied systematically to diagnose problems. Your knowledge and skill may be called upon only after a user or an operator has already attempted some problem solving (e.g., based upon error messages displayed directly to the screen) and then submitted a trouble ticket. The effectiveness of your troubleshooting is maximized by:

- thorough documentation of the problem.
  - date/time of problem occurrence.
  - hardware/software.
  - initiating conditions.
  - symptoms, including log entries and messages on GUIs/screens.
- verification.
  - identify/review relevant publications (e.g., COTS product manuals, ECS tools and procedures manuals).
  - replicate problem.
- identification.
  - review product/subsystem logs.
  - review HP OpenView Event Browser.
- analysis.
  - detailed event review (e.g., logs, HP OpenView Event Browser Event Fields).
  - troubleshooting procedures.
  - determination of cause/action.

ECS Assistant vs. HP OpenView

The HP OpenView system provides a very powerful dynamic, real-time monitoring capability. However, HP OpenView works only with SNMP event data. ECS logs may capture a wider range of events. The ECS Assistant was added to provide an additional easy-to-use tool that has a log viewing and system monitoring capability to view server logs. Figure 5 shows the main ECS Assistant GUI, and Figure 6 shows the ECS Assistant subsystem manager GUI.

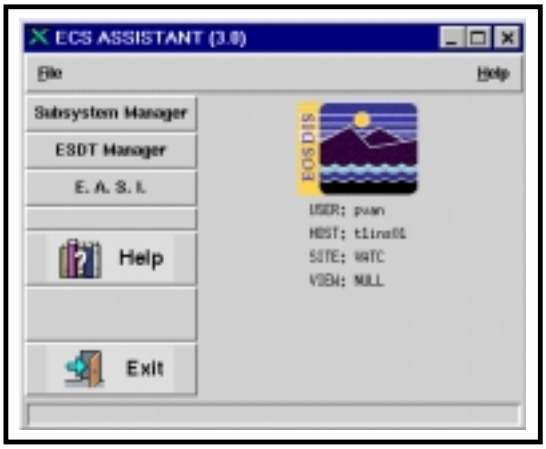


Figure 5. ECS Assistant GUI

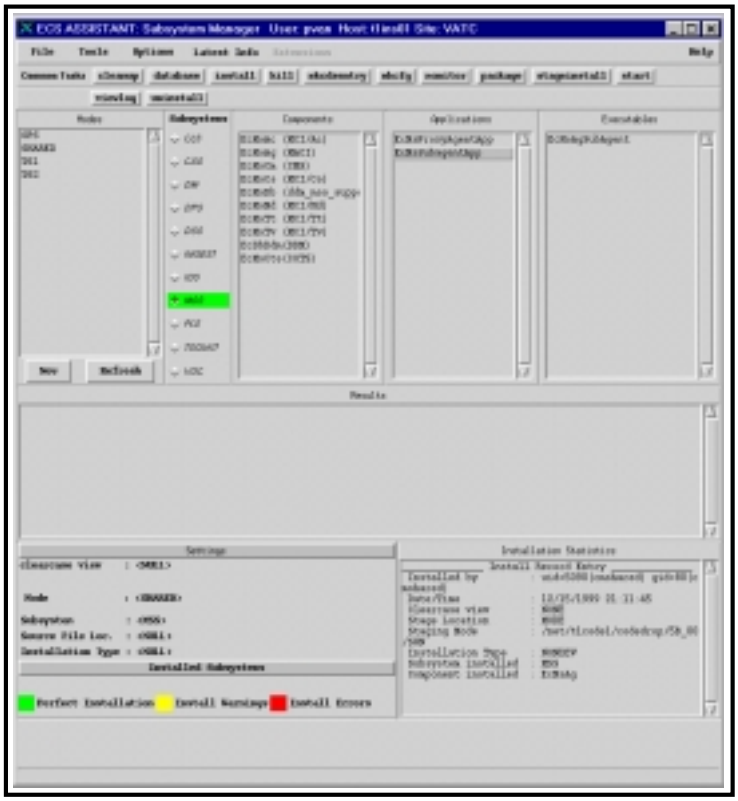


Figure 6. ECS Assistant Subsystem Manager GUI

To run the ECS Assistant, use the following procedure.

Starting ECS Assistant

1 Log in to one of the host machines.

2• At the UNIX prompt on the host from which the ECS Assistant is to be run, type **setenv ECS_HOME /usr/ecs**, and then press the **Return/Enter** key.

- To verify the setting, type **echo $ECS_HOME**, and then press the **Return/Enter** key.

3• If necessary, at the UNIX prompt on the host from which the ECS Assistant is to be run, type **cleartool setview *ViewName***, and then press the **Return/Enter** key.

- The ***ViewName*** is the ClearCase view to be used while the ECS Assistant is running in this session. For example, type **cleartool jdoe**, and then press the **Return/Enter** key.
- A ClearCase view is required only if the ECS Assistant needs to be able to "see" into a ClearCase VOB; a view is not necessary otherwise.

4• At the UNIX prompt, type **cd /tools/common/ea**, and then press the **Return/Enter** key. Then type **EcCoAssist &**, and then press the **Return/Enter** key.

- **/tools/common/ea** is the path where ECS Assistant is installed.
- The ECS Assistant GUI is displayed.

5 At the ECS Assistant GUI, click the **Subsystem Manager** pushbutton.

- The Subsystem Manager GUI is displayed.

6 Select a mode by clicking a mode in the mode listing.

- Once the mode is selected, the color of the subsystem name list is changed.

7 Select a subsystem with the **Subsystem** radio button.

- The component list for the selected subsystem will appear in the component window.

8 Select a component by clicking the component name under the component window.

- The selected component will be highlighted.
- The server list corresponding to that component will appear in the server window.

ECS Assistant provides a convenient way to monitor the status of the servers by listing their up/down condition. The status flag for a server is up or down indicating whether or not that server is running. Two GUI screens are used; these are the **Server Monitor**, shown in Figure 7, and the **cdsping** window, shown in Figure 8.

Figure 7. ECS Assistant Server Monitor

Figure 8. ECS Assistant cdsping GUI

To start up the ECS Assistant Server Monitor GUI, use the following procedure.

Using the ECS Assistant Server Monitor

1 At the ECS **Subsystem Manager** GUI, select a mode by clicking a mode in the mode list.

- Once the mode is selected, the color of the subsystem name list is changed.

2 Select a subsystem by clicking the radio button next to the subsystem name under the subsystem component window.

- The selected subsystem radio button is highlighted.
- The components corresponding to that the subsystem are displayed in the component window.

3 Select a component by clicking its name under the component window.

- All the servers for the selected component are displayed in the server window.

4 If desired, click the **monitor** button from the common tasks window.

- The ECS Assistant **Server Monitor** window is displayed.
- The status "**UP/DOWN**" indicates whether the server is running.

5 To see which host each server is running on, click the **cdsping all servers…** button.

- The ECS Monitor (**cdsping**) GUI is displayed.
- The host name for each running server is listed

6 Both the **Server Monitor** and **cdsping** GUI can be updated by clicking the **update** button in the GUI.

- This causes the list to update to the current status.

7 To monitor other servers, repeat steps 2-4.

8 To exit, click the **EXIT** button.

- This terminates display of the monitor GUI.

Analysis/Troubleshooting: COTS Hardware

The ECS hardware is composed almost entirely of commercial, off-the-shelf (COTS) products, for which there are vendor maintenance warranties and/or COTS hardware support contracts. When a system problem is discovered, there is an initial troubleshooting/diagnostics procedure to be followed which is generic – i.e., not limited to hardware problems. However, when a hardware problem is indicated, the procedure refers the problem to the Maintenance Coordinator for hardware corrective maintenance. System troubleshooting tools and principles apply:

- HP OpenView for quick assessment of status.
- HP OpenView Event Log Browser for sequence of events.
- Initial troubleshooting.
  - Review error message against hardware operator manual.
  - Verify connections (power, network, interface cables).
  - Run internal systems and/or network diagnostics.
  - Review system logs for evidence of previous problems.
  - Attempt system reboot.
  - If problem is hardware (e.g., software has been working and reboot is unsuccessful), report it to the Maintenance Coordinator – i.e., refer problem for preparation of a maintenance Work Order in Inventory/Logistical Management (ILM) software.

The ILM Tool

The ILM tool is one application of XRP-II (the other is Baseline Manager. The main screen of XRP-II, illustrated in Figure 9, permits access to four menus (*Note*: Depending on the access level established for you by the XRP-II administrator, you may not have access to all of the menus):

- **Baseline Management** menu provides access to functions for maintaining control item and bill of material information.
- **ILM Main Menu** provides access to functions for Inventory/Logistical Management (ILM) services, including entry and management of EIN (Equipment Identification Number) information and management of the EIN structure for the ECS inventory, as well as entry of maintenance Work Orders and other maintenance records.
- **System Utilities Menu** provides access to functions for maintaining information that spans functional domains, and for importing and exporting records.
- **System Tools** menu provides access to functions for managing the security, health, and configuration of XRP-II.

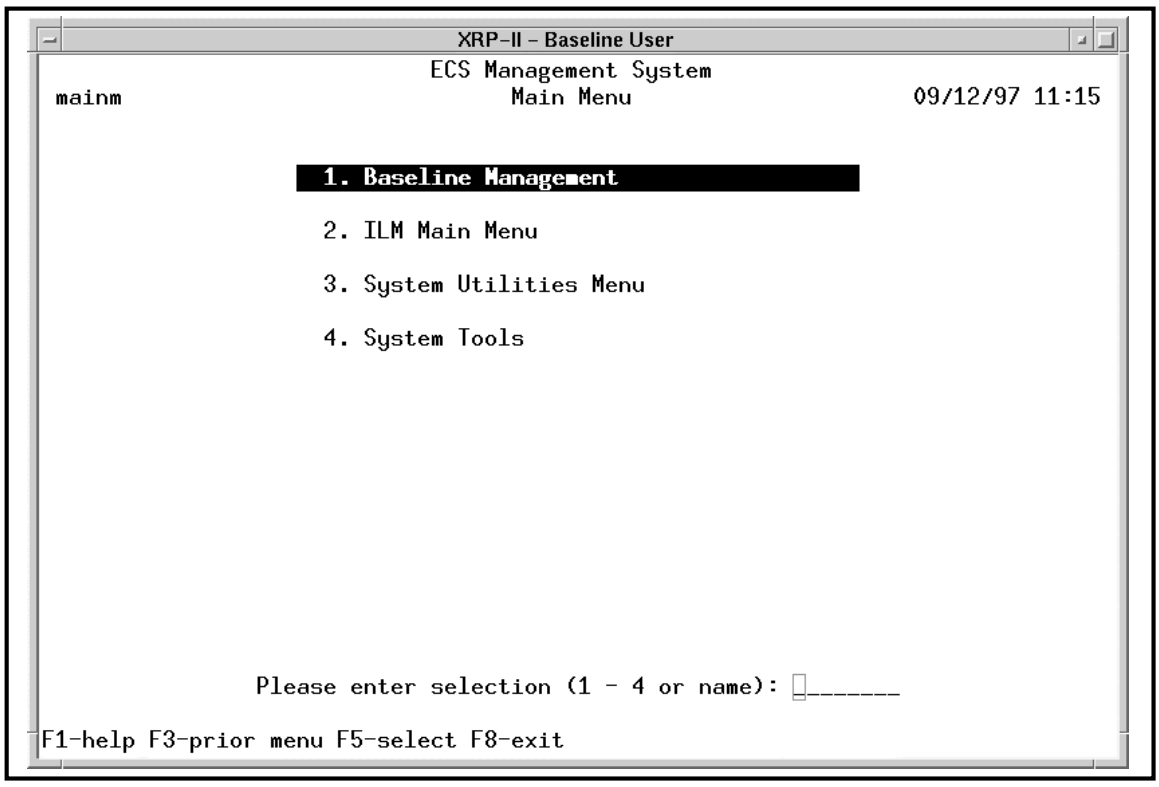


Figure 9. XRP-II Main Menu Screen for Baseline Manager and Inventory/Logistical Management.

The user interface for XRP-II is a Character User Interface (CHUI). The various screens are accessible through navigation of a hierarchical menu structure. Figure 10 illustrates that structure for ILM. Data concerning maintenance actions can be added, modified, or deleted by selecting an appropriate data entry screen from the Maintenance Menu. Data entry screens permit modification of the master file (or catalog) that describes maintenance actions individually. Each screen accesses a particular set of records and contains a unique set of fields corresponding to an item's class. All screens function in essentially the same way, and use bottom-line commands such as those shown in the **Work Order Entry** screen illustrated in Figure 13. A bottom-line command is executed by typing its first letter, or, in the case of those preceded by a slash (/), by typing the slash and the first letter.

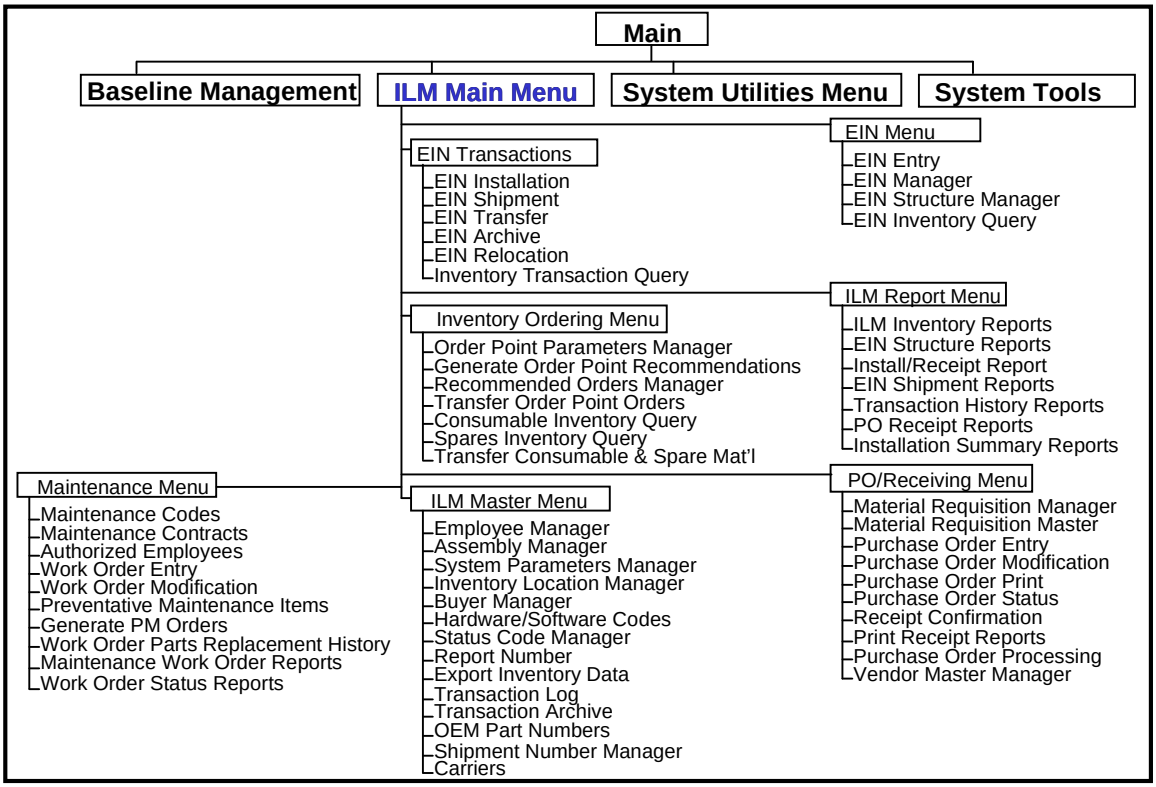


Figure 10. XRP-II Hierarchical Menu Structure for ILM.

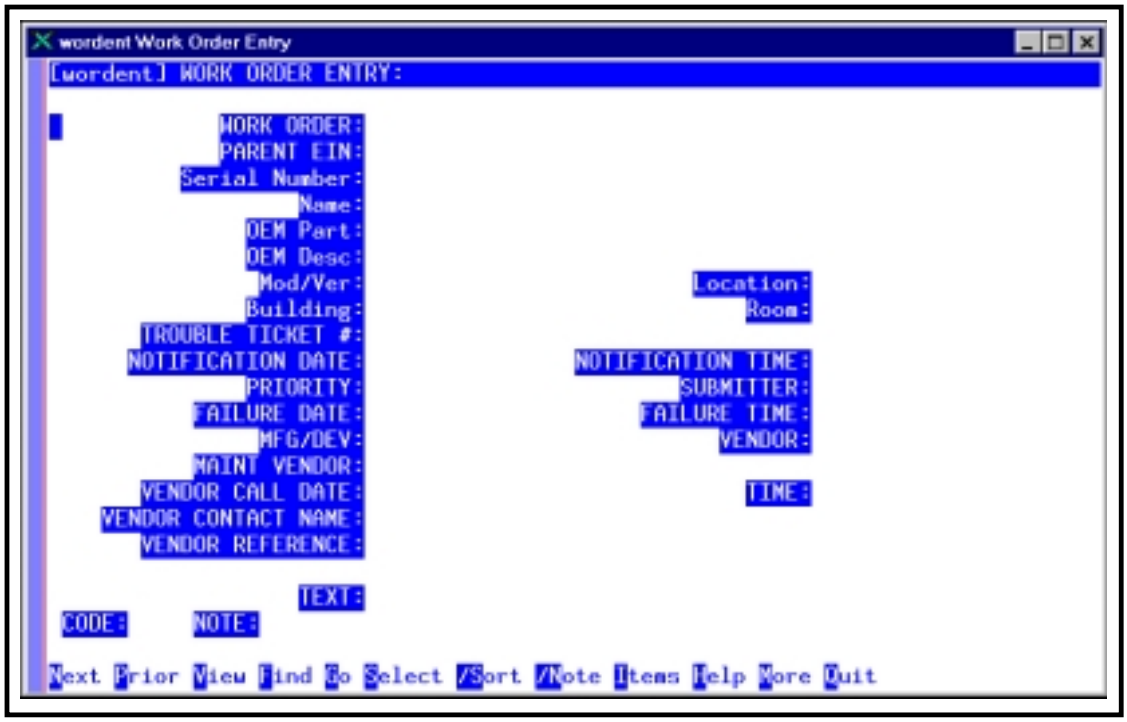


Figure 11. ILM Work Order Entry Screen.

A problem that is not resolved through initial troubleshooting will often require troubleshooting teamwork by the Maintenance Coordinator, the System Administrator, and perhaps a Network Analyst. These troubleshooters may perform additional steps to resolve the problem:

- specific troubleshooting procedures described in COTS hardware manuals.
- non-replacement intervention (e.g., adjustment).
- replace hardware with maintenance spare.
  - locally purchased (non-stocked) item.
  - installed (hot-swappable, excess capacity) spares (e.g., RAID storage, power supplies, network cards, tape drives).

If the hardware problem is not resolved by the actions of the local staff, it may be necessary to request assistance through the Maintenance Coordinator from a maintenance contractor for on-site hardware support. Suppose, for example, that you are a Maintenance Coordinator and HP OpenView has indicated a problem with one of the Sun workstations, that initial troubleshooting finds the workstation to be inoperable, that a hardware problem report has been forwarded to you, and that you and System Administrator cannot resolve the problem through additional troubleshooting. That workstation is hard down. The correct approach is:

- Organize the data on the problem and use ILM software to prepare a maintenance Work Order.
- Call the support provider's technical support center to obtain on-site assistance.
  - Provide them with the background data.
  - Obtain a case reference number from them.
  - Update the ILM record to reflect the time and date of the call and the case number.
  - Notify the originator of the problem that the contractor is on the way.
- Arrange for site access for the maintenance technician.
  - Record arrival time.
  - Escort technician to hardware.
  - Assist in problem resolution (e.g., arrange equipment shutdown, demonstrate problem).
  - Obtain any needed technical references that are available at the site.
- Update the ILM record with actions taken to correct the problem and delay time experienced for the repair, including start/stop times and reasons for each delay

- For any replaced part, update the ILM record with additional supporting data (Work Order Parts Replacement History).
  - Part number of the new item.
  - Serial numbers of the old and new items.
  - Equipment Identification Number (EIN) assigned to the new item (if applicable).
  - Model number of replacement Line Replaceable Unit (LRU). [Note: If the model number of the replacement LRU is different from the part removed, a configuration change request (CCR) is required for configuration management.]
  - Name of the item replaced.

The following procedures are applicable to help you implement this approach.

In preparation to request on-site hardware support from the maintenance contractor to repair the down Sun workstation, use the following procedure to obtain the background information needed.

Obtaining On-Site Hardware Support: Background Information

1 Collect information needed to obtain contract maintenance support.

- Obtain **make**, **model**, **serial number**, and **location** of the failed system from the hardware database.
- Obtain description of problem and symptoms from the **problem report**.
- Identify the **criticality** of the COTS hardware experiencing the problem.

2 Determine maintenance provider data.

- Obtain **name**, and **telephone number** of the maintenance provider.
- Obtain **access code** needed to obtain support.
- Obtain **telephone number** of the support provider's technical support center.
- Obtain **name** of site authorized contact person.

Once you have collected the background information you need to contact the maintenance vendor, make the contact and then enter a Work Order record into the ILM tool. Use the following procedure.

Use ILM to Prepare a Maintenance Work Order

1 On workstation ***x*0mss##**, at the UNIX prompt in a terminal window, type **ilmusr <*ipaddress*> xterm** at a UNIX command prompt and then press the **Return** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL; the **##** will be an identifying two-digit number (e.g., **e0mss02** indicates a management services subsystem workstation at EDC).
- A script is executed which determines the operator's terminal type from the environment, prompts for a terminal ID, and establishes a Baseline Manager/ILM operating environment. XRP-II is then started and the **Main Screen** is displayed.

2 Type the number **2** (for **ILM Main Menu**) and press the **Return/Enter** key.

- The **ILM Main Menu** screen is displayed.

3 Type the number **6** (for **Maintenance Menu**) and press the **Return/Enter** key.

- The **Maintenance Menu** screen is displayed.

4 Type the number **1** (for **Work Order Entry**) and press the **Return/Enter** key.

- The **Work Order Entry** CHUI screen is displayed, with the cursor at the **Work Order:** field; the screen is in the **ADD** mode.

5 Press the **Return/Enter** key.

- The system generated **WORK ORDER ID** is displayed in the text field and the cursor moves to the **PARENT EIN:** field.

6 Type the EIN of the parent item, and then press the **Return/Enter** key.

- The typed entry is displayed in the **PARENT EIN:** field, and data from the EIN file for the parent are displayed in the **Serial Number:**, **Name:**, **OEM Part:**, **OEM Desc:**, **Location:**, **Building:**, and **Room:** fields. Initial values (which may be changed) are displayed in the **NOTIFICATION DATE:**, **NOTIFICATION TIME:**, **MFG/DEV:**, **VENDOR:**, and **MAINT VENDOR:** fields.
- As an option instead of typing the EIN of the parent, the operator may type **/Z** and zoom out to the EIN list, scroll to the desired EIN, type **t** to tag the desired EIN, and then type **Q** (for **Quit**) to make the entry and populate the associated fields.
- The cursor is displayed in the **TROUBLE TICKET:** field.

7 If applicable, type the identification number of an associated trouble ticket (e.g., if a trouble ticket was initially prepared for the problem), and then press the **Return/Enter** key.

- The field may be bypassed by just pressing the **Return/Enter** key.
- The typed entry is displayed in the **TROUBLE TICKET:** field and the cursor is displayed in the **NOTIFICATION DATE:** field.

8 Type the date (using format mm/dd/yy) on which notification of the problem was received and then press the **Return/Enter** key.

- To bypass the field, leaving the displayed current date, just press the **Return/Enter** key.
- The typed entry is displayed in the **NOTIFICATION DATE:** field, and the cursor is displayed in the **NOTIFICATION TIME:** field.

9 Type the time (using format hh:mm) at which notification of the problem was received and then press the **Return/Enter** key.

- To bypass the field, leaving the displayed current time, just press the **Return/Enter** key.
- The typed entry is displayed in the **NOTIFICATION TIME:** field, and the cursor is displayed in the **PRIORITY:** field.

10 Type a priority consistent with local policy and assessment (e.g., in this exercise, type **1**), and then press the **Return/Enter** key.

- The typed entry is displayed in the **PRIORITY:** field, and the cursor is displayed in the **SUBMITTER:** field.

11 Type your employee code number and then press the **Return/Enter** key.

- The typed entry is displayed in the **SUBMITTER:** field, and the cursor is displayed in the **FAILURE DATE:** field.
- As an option instead of typing the employee code number, the operator may type **/Z** and zoom out to a list of code numbers and employees, scroll to the desired entry, type **t** to tag the desired entry, and then type **Q** (for **Quit**) to make the entry.

12 Type the actual failure date (using format mm/dd/yy), and then press the **Return/Enter** key.

- The typed entry is displayed in the **FAILURE DATE:** field and the cursor is displayed in the **FAILURE TIME:** field.

13 Type the actual failure time (using format hh:mm), and then press the **Return/Enter** key.

- The typed entry is displayed in the **FAILURE TIME:** field, and the cursor is displayed in the **MFG/DEV:** field.

14 Type the ID of the manufacturer or developer, and then press the **Return/Enter** key.

- The typed entry is displayed in the **MFG/DEV:** field, and the cursor is displayed in the **VENDOR:** field.
- As an option instead of typing the ID, the operator may type **/Z** and zoom out to a list of manufacturers/developers, scroll to the desired entry, type **t** to tag the desired entry, and then type **Q** (for **Quit**) to make the entry. *Note*: This option is only available if the information has previously been entered using the Vendor Master Maintenance screen.

15 Type the code for the vendor from whom the item was purchased and then press the **Return/Enter** key.

- The typed entry is displayed in the **VENDOR:** field, and the cursor is displayed in the **MAINT VENDOR:** field.

16 Type the ID of the maintenance vendor, and the press the **Return/Enter** key.

- The typed entry is displayed in the **MAINT VENDOR:** field, and the cursor is displayed in the **VENDOR CALL DATE:** field.
- As an option instead of typing the ID, the operator may type **/Z** and zoom out to a list of maintenance vendors, scroll to the desired entry, type **t** to tag the desired entry, and then type **Q** (for **Quit**) to make the entry. *Note*: This option is only available if the information has previously been entered using the Vendor Master Maintenance screen.

17 Type the date (using format mm/dd/yy) on which the vendor was called and informed of the problem, and then press the **Return/Enter** key.

- The typed entry is displayed in the **VENDOR CALL DATE:** field and the cursor is displayed in the **TIME:** field.

18 Type the time (using format hh:mm) at which the vendor was called and informed of the problem, and then press the **Return/Enter** key.

- The typed entry is displayed in the **TIME:** field, and the cursor is displayed in the **VENDOR CONTACT NAME:** field.

19 Type the name of the person who was contacted at the vendor, and the press the **Return/Enter** key.

- The typed entry is displayed in the **VENDOR CONTACT NAME:** field, and the cursor is displayed in the **VENDOR REFERENCE:** field.

20 Optional: Type any desired information in reference to the vendor (up to 20 characters), and then press the **Return/Enter** key.

- The entry may be bypassed by just pressing the **Return/Enter** key.
- The typed entry is displayed in the **VENDOR REFERENCE:** field, and the cursor is displayed in the **TEXT:** field.

21 Type **/z** to open a free-form text window, then type any pertinent details on the failure or repair. (*Note*: To keep the entered text visible, press the **Return/Enter** key when the cursor reaches the edge of the screen during typing of each line.) Press the **F3** key to exit when done.

- The free-form text window is closed, the notation **T** is displayed in the **TEXT:** field, and the cursor is displayed in the **CODE:** field.

22 Optional: Type any desired two-character code that has been established for identified specific needs, and then press the **Return/Enter** key.

- This field may be bypassed by just pressing the **Return/Enter** key.
- The typed entry is displayed in the **CODE:** field, and the cursor is displayed in the **NOTE:** field.

23 Optional: Type any desired note (up to 60 characters) to be added to the Work Order, and then press the **F3** key to exit.

- The typed entry is displayed in the **NOTE:** field, and the **ADD** mode is terminated. (*Note*: If you have pressed the **Return/Enter** key instead of the **F3** key, the screen remains in the **ADD** mode and the cursor is displayed at the top in the **WORK ORDER:** field; you must press the **F3** key to exit.)

When the **Work Order Entry** screen is exited, the system copies all active children for the parent EIN into the work order. The operator then uses the **Work Order Modification** screen to record and track details about the failure.

- Main **Work Order Modification** screen is used to record down times, and, when a vendor service call is complete, the vendor times and any appropriate notes.
- The **Items** pages accessible from the **Work Order Modification** screen are used to designate which item(s) failed, and any new replacement parts, as well as accompanying notes.

Suppose that the vendor was called and has made a service call lasting one hour to isolate and repair the problem for which you created a maintenance Work Order entry. The problem was isolated to one of the children of the parent EIN, which was replaced to complete the repair. Use the following procedure to document the down time and service call.

Use ILM to Prepare a Maintenance Work Order Modification

1 On workstation ***x*0mss##**, at the UNIX prompt in a terminal window, type **ilmusr <*ipaddress*> xterm** at a UNIX command prompt and then press the **Return** key.

- NOTE: The ***x*** in the workstation name will be a letter designating your site: **g** = GSFC, **m** = SMC, **l** = LaRC, **e** = EDC, **n** = NSIDC, **o** = ORNL, **a** = ASF, **j** = JPL; the **##** will be an identifying two-digit number (e.g., **e0mss02** indicates a management services subsystem workstation at EDC).
- A script is executed which determines the operator's terminal type from the environment, prompts for a terminal ID, and establishes a Baseline Manager/ILM operating environment. XRP-II is then started and the **Main Screen** is displayed.

2 Type the number **2** (for **ILM Main Menu**) and press the **Return/Enter** key.

- The **ILM Main Menu** screen is displayed.

3 Type the number **6** (for **Maintenance Menu**) and press the **Return/Enter** key.

- The **Maintenance Menu** screen is displayed.

4 Type the number **2** (for **Work Order Modification**) and press the **Return/Enter** key.

- The **Work Order Modification** CHUI screen (form) is displayed, with the cursor at the **Work Order:** field; the screen is in the **QUERY** mode.

5 Type **V** (for **View**) to toggle the view to the list of work orders.

- The list of work orders is displayed, with the cursor at the Work Order identification of the first item in the list.

6 Use the arrow keys to scroll down the list to the entry for the Work Order you previously entered.

- If necessitated by a very long list, you may type **N** (for **Next**) to scroll down a page at a time; typing **P** (for **Prior**) scrolls up a page at a time.
- If you know the identifier for the Work Order you want to modify, you may type **F** (for **Find**), which displays an entry field into which you can type the identifier. Then press the **F5** key to initiate the Find action. It is possible to search on other columns by pressing the **Return/Enter** key after typing **F** and before typing the search item.

7 When the cursor is in the line for the desired Work Order entry, type **V** (for **View**) to toggle back to the form display.

- The Work Order Modification form is displayed with data for the selected Work Order entry.

8 Repeatedly press the **Return/Enter** key to move the cursor through the form until it is displayed in the **VENDOR ARRIVE DATE:** field.

- The cursor is displayed in the **VENDOR ARRIVE DATE:** field.

9 Type **/M** (for **Modify**).

- The screen shows the **MODIFY** mode menu at the bottom, indicating **MODIFY** mode.

10 Type the date (using format mm/dd/yy) on which the vendor arrived and then press the **Return/Enter** key.

- The typed entry is displayed in the **VENDOR ARRIVE DATE:** field, and the cursor is displayed in the **VENDOR ARRIVE TIME:** field.

11 Type the time (using format hh:mm) at which the vendor arrived and then press the **Return/Enter** key.

- The typed entry is displayed in the **VENDOR ARRIVE TIME:** field, and the cursor is displayed in the **VENDOR COMPLETE DATE:** field.

12 Type the date (using format mm/dd/yy) on which the vendor completed the repair and then press the **Return/Enter** key.

- The typed entry is displayed in the **VENDOR COMPLETE DATE:** field, and the cursor is displayed in the **VENDOR COMPLETE TIME:** field.

13 Type the time (using format hh:mm) at which the vendor completed the repair and then press the **Return/Enter** key.

- The typed entry is displayed in the **VENDOR COMPLETE TIME:** field, and the cursor is displayed in the **MFG/DEV:** field.

14 Press the **Return/Enter** key repeatedly until the cursor is displayed in the **NOTE:** field.

- The cursor is displayed in the **NOTE:** field.

15 Type **/N** (for **Note**).

- A free-text field is displayed.

16 Type any pertinent notes to document events related to the failure and repair.

- The typed entry is displayed in the free-text entry area.

17 Press the **F3** key to exit the free-text entry area.

- The free-text entry area is closed and the cursor is displayed in the **NOTE:** field.

18 Press the **Return/Enter** key repeatedly until the cursor is displayed in the first **START DATE:** field.

- T he cursor is displayed in the first **START DATE:** field.

19 Type the date on which the system failure was first noted, and then press the **Return/Enter** key.

- The typed entry is displayed in the **START DATE:** field, and the cursor is displayed in the first **END DATE:** field.

20 Type the date on which switchover (if applicable) or repair began (i.e., the end of Administrative and Logistics Delay Time -- ALDT), and then press the **Return/Enter** key.

- The typed entry is displayed in the first **END DATE:** field, and the cursor is displayed in the first **START TIME:** field.

21 Type the time at which the system failure was first noted, and then press the **Return/Enter** key.

- The typed entry is displayed in the first **START TIME:** field, and the cursor is displayed in the first **END TIME:** field.

22 Type the time at which switchover (if applicable) or repair began (i.e., the end of ALDT), and then press the **Return/Enter** key.

- The typed entry is displayed in the first **END TIME:** field, and the cursor is displayed in the first **REASON:** field.

23 Type the code identify the reason for the first down time entry, and then press the **Return/Enter** key.

- If desired, you may type **/Z** (for **Zoom**) to display a list of reason codes. You may then use the down arrow key to scroll down the list to the desired code, type **T** to tag the entry, and then type **Q** (for **Quit**) to enter the code in the **REASON:** field.

- The typed (or selected) entry is displayed in the **REASON:** field, and the cursor is displayed in the next **START DATE:** field.

24 Repeat steps **19 - 23**, using as many Time-Date-Reason blocks as applicable and necessary, to enter starting and ending dates, times, and reason codes for additional down time attributable to repair activities, switchover activities, and total chargeable down time, respectively.

- The time and reason data are displayed in the appropriate fields. When the **Return/Enter** key is pressed in the last **REASON:** field, the **QUERY** mode menu is displayed at the bottom of the screen, and the cursor remains in the **REASON:** field.

25 Type **R** (for **Right**).

- The screen display shifts to show the **Chargeable Hours** page, and the cursor is displayed in the **Work Order:** field.

26 Press the **Return/Enter** key.

- The cursor is displayed in the **ALDT:** field.

27 Type **/M** (for **Modify**).

- The screen shows the **MODIFY** mode menu at the bottom, indicating **MODIFY** mode.

28 Type the number of hours chargeable to ALDT, and then press the **Return/Enter** key.

- The typed entry is displayed in the **ALDT:** field, and the cursor is displayed in the **TIME TO REPAIR:** field.

29 Type the number of hours chargeable to the repair, and then press the **Return/Enter** key.

- The typed entry is displayed in the **ALDT:** field, and the cursor is displayed in the **SWITCHOVER TIME:** field.

30 If applicable, type the number of hours chargeable to switchover activities, and then press the **Return/Enter** key.

- The typed entry is displayed in the **SWITCHOVER TIME:** field, and the cursor is displayed in the **TOTAL CHARGEABLE DOWNTIME:** field.

31 Type the total number of hours of down time, and then press the **Return/Enter** key.

- The typed entry is displayed in the **TOTAL CHARGEABLE DOWNTIME:** field, the **QUERY** mode menu is displayed at the bottom of the screen, and the cursor remains in the **TOTAL CHARGEABLE DOWNTIME:** field.

32 Type **I** (for **Items**).

- The items page is displayed for the first child item of the parent EIN, with the cursor positioned at the **COMPONENT EIN:** field.

33 To record the replacement of the item, repeatedly type **N** (for **Next**) until the page for the replaced item is located.

- If there are a large number of child items, the location of the desired item may be facilitated by typing **V** (for **View**) to toggle to the list view. Then use the arrow keys to scroll through the list to locate the item and type **V** again to display the form for that item.

34 Repeatedly press the **Return/Enter** key until the cursor is displayed in the **REPLACE (R) OR NEW (N):** field.

- The cursor is displayed in the **REPLACE (R) OR NEW (N):** field.

35 Type **/M** (for **Modify**).

- The screen shows the **MODIFY** mode menu at the bottom, indicating **MODIFY** mode.

36 Type **R**, and then press the **Return/Enter** key.

- The typed entry is displayed in the **REPLACE (R) OR NEW (N):** field, and the cursor is displayed in the **REPLACE OR ADD DATE:** field.

37 Type the date (using format mm/dd/yy) on which the replacement was made, and then press the **Return/Enter** key.

- The typed entry is displayed in the **REPLACE OR ADD DATE:** field, and the cursor is displayed in the **RECORD EVENTS:** field.

38 Type **/Z** (for **Zoom**).

- A free-text entry field is displayed.

39 Type failure/repair details in the free-text entry field, and press the **F3** key when done.

- The free-text entry field is closed, a **T** is displayed in the **RECORD EVENTS:** field to indicate that text has been entered, and the **QUERY** mode menu is displayed at the bottom of the screen.

40 Type **Q** (for **Quit**).

- The ILM Maintenance menu is displayed.

In unusual cases, it may be necessary to resort to non-standard hardware support procedures. In the event that the maintenance contractor's assigned technician is not providing timely successful repair, or if the maintenance action is otherwise unsatisfactory, it may be necessary to escalate the problem to bring it to the attention of the support contractor's management. The escalation is achieved by calling the maintenance contractor's technical support center and providing them with the case reference number. Another non-standard support approach, which may be costly and is to be used only as a last resort for mission-critical repairs, is Time and Material (T&M) support. For T&M support, the local Maintenance Coordinator must obtain authorization from the ILS Maintenance Coordinator or, if that person is unavailable, from the Sustaining Engineering Organization (SEO).

Failover/Switchover

In the ECS context, "failover" refers to the configuration of a fall-back platform for key system components (e.g., Ingest Server) permitting switchover to that platform to recover key functionality in a reasonably short period of time in the event of loss of the primary platform. The switchover capability can also be used to switch to the backup server operation for maintenance or software upgrade purposes. After repair of the primary platform, control is switched back from the normally secondary platform to the normally primary platform ("failback"). In the case of Ingest, for example, the ICL hardware consists of one pair of SGI servers (Ingest Server). One server in the pair acts as the "hot" server, and the other is a "warm" standby backup. The Redundant Array of Inexpensive Disks (RAID) device between the two servers is dual ported to both machines (each machine "sees" the entire RAID), but only one of the hosts (the **primary**) is actively addressing the RAID at any one time. Figure 12 illustrates the concept in the context of the Ingest subsystem.

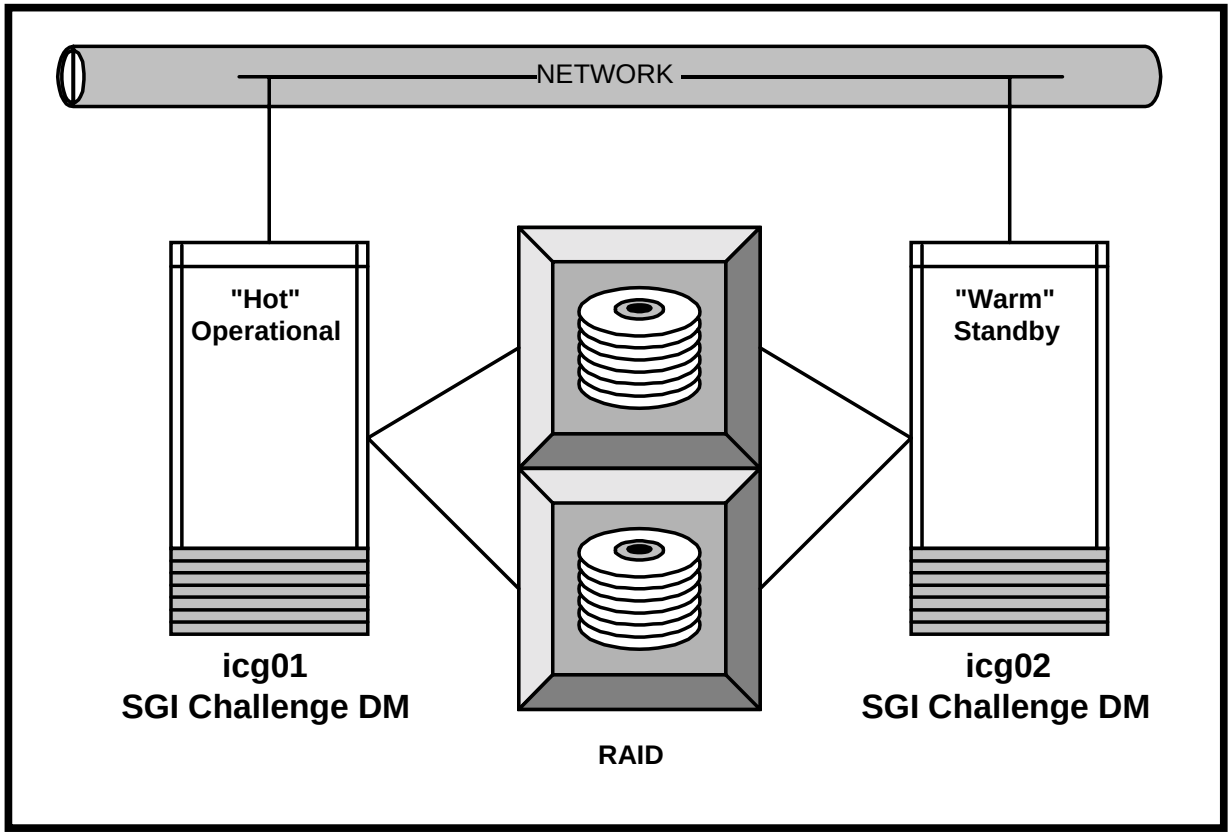


Figure 12. "Failover" concept.

For the implementation of the failover scheme, aside from the dual physical connection of the RAID, a number of specific changes are made to the host system, network, and peripheral device configuration. The result is that a *virtual ip* is established for the host, so that the ip address for the host can be the same regardless of which physical platform has RAID control.

In the procedure for executing the switchover, a script on the secondary host establishes control (e.g., takes ownership of the RAID, remounts partitions, recovers the database) and a script on the MSS File Server cleans up Cell Directory Service (CDS) entries. The procedure may require switching the HiPPI connection (e.g., the EDC DAAC uses HiPPI connection with Ingest, and so for Ingest "Failover" at EDC, the HiPPI connection must also be switched). Switchover also entails flushing of the Address Resolution Protocol (ARP) tables in the local and external interface routers, as well as starting the Subagent and ECS custom code on the backup platform. The following procedure may be used to illustrate switchover. The example uses the Ingest context, but the procedure is generic and applicable for hosts other than Ingest.

Switchover from Primary Host to Backup Host

1 Upon indication of failure of a primary host (e.g., on the HP OpenView network display, the icon for the Ingest host ***x*0icg01** turns red), log in to the backup host (e.g., for Ingest, **e0icg02**, **g0icg02**, **l0icg02**); log in as **root**.

2 Execute the failover script on the backup host (e.g., to execute the failover script on the Ingest backup, type **/failover/scripts/failover_to_icg02** and then press the **Return/Enter** key).

- The script execution gives RAID control to the secondary host.
- ***Note***: For maximum efficiency, do not wait for completion of a step before proceeding; proceed immediately to the next steps unless the procedure directs otherwise.

3 Initiate clearing of the ARP cache in the Ebnet router by calling the Communications Manager (e.g., at GSFC, call 301-286-6141), with the request (an appropriate request for Ingest is: *"This is* <name>, <position title> *at ECS and we are going to our backup Ingest host; to support this, we need the IPNOC to clear the ARP cache in router* <router name>. *Please advise us when this has been accomplished. My phone number is* <phone number>. *My pager number (if any) is* <pager number>*."*

- ***Note***: Router name is **er32-1** (GSFC), **larc-gw1** (LaRC), or **edc-gw1** (EDC).

4 Initiate clearing of the ARP table in the PowerHub 8000 by calling the on-duty network administrator with the request.

- The network administrator will log in to the router as **root**, enter the <***password***>, then enter **ip arp clear**, and finally enter **bye**.

5 Log in as **root** to the MSS File Server host (e.g., **e0mss01**, **g0mss10**, **l0mss10**)

6 Execute the appropriate failover script on the MSS File Server (e.g., to execute the failover script for Ingest, type **/tools/admin/scripts/Failover_to_<*x*>icg02_CDS.sh** and then press the **Return/Enter** key).

- The script execution cleans up the CDS entries.

7 **For failover of SGI hosts attached to the HiPPI network** (otherwise, go to Step 8), execute the HiPPI switchover as follows (***Note***: EDC is the only DAAC that currently uses the HiPPI connection with Ingest):

- Ensure that the HiPPI interface is disabled on the primary host. If the host is down, the port will be disabled; otherwise, log in to the host as **root** and execute the command **hipcntl hip0 reject**.
- Log in to the HiPPI switch (telnet or connected terminal).
- Become **"system"** user.
- Execute command **set huntgroup <n_1> <n_2>**.
  - ***Note***: n_1 and n_2 are numbers unique to ECS sites and hosts; refer to Appendix A of *ECS Failover Design*, Document 920-xx-xxx-xxx for the numbers needed for the specific site and host/subsystem.
- Execute command **save h**.
- Log off HiPPI switch.
- Log in to the secondary host as **root** and re-configure its HiPPI interface to assume the IP address of the primary host by executing the command **ifconfig hip0 inet <*ip address*>**.
  - ***Note***: ***ip address*** is the site- and host-unique "virtual" IP address established for the primary host to enable the failover/switchover to occur; refer to Appendix A of *ECS Failover Design*, Document 920-xx-xxx-xxx for the IP address needed for the specific site and host/subsystem.

8 Before proceeding to Step 9, verify successful hardware switchover, as follows:

- Verify that the completion message was issued at the end of Step 2.
- To verify that the L0_buffer and data2 file systems were successfully mounted on the secondary host, on that host type **df -kl** and then press the **Return/Enter** key; the returned display should be similar to the following.

```
Filesystem          Type    kbytes      use       avail     %use  Mounted on
/dev/root           xfs     3913496     2344612   1568884   60    /
/dev/dsk/xlv/buffer xfs     137775872   74247840  63528032  54    /L0_buffer
/dev/dsk/xlv/data2  xfs     4097740     2557500   1540240   63    /data2
/dev/dsk/xlv/data   xfs     8950996     1628004   7322992   19    /data1
```

- To verify that the l0buffer is exported, on the secondary host enter the command **exportfs**: the returned display should be similar to the following:

```
/L0_buffer/OPS/icl
/L0_buffer/TS1/icl
/L0_buffer/TS2/icl
```

- Verify that Sybase is running on the secondary host. (e.g., have the Database Administrator type **isql -U<*username*> -P<*password*> -S<*servername_srvr*>** and verify that prompt **>1** appears; type **quit** to exit).
- Verify the ability to log in to the virtual host from another platform (e.g., from remote platform, use the **ssh <*x*>vicgaa.<*daac*>b.ecs.nasa.gov** command and log in to the virtual host).
- To verify that swap space is available on the new primary, type **swap -ln** and then press the **Return/Enter** key; the return should be similar to the following:

```
# path                    pri     pswap    free    maxswap      vswap
 2 /dev/dsk/dks1d3s1      3       2.10g    2.06g   2.10g        0.00k
 1 /dev/swap              0       512.00m  2.56m   512.00m      0.00k
g0icg02{pvan}[2]->
```

9 With hardware failover to the new primary host now completed, start the Subagent (i.e., enter the command **/usr/ecs/SHARED/CUSTOM/utilities/EcMsAgStartSubagent SHARED**) and, if desired, use HP OpenView to start ECS Custom code on the host [refer to the procedure **Start an Application/Program** (Document 611-CD-510-001, Section 7.3.2)].

Once the system is operational again with the backup supporting the virtual IP address, it is necessary to boot the primary in standalone mode (i.e., single-user mode) and immediately execute the script **/failover/scripts/dead_boot.<*host_type*>** (e.g., for Ingest, execute **/failover/scripts/dead_boot.icg**). This script disables ip aliasing and disables launching of Sybase at startup. After the script is run, the primary host can be returned to multiuser mode and hardware troubleshooting/repair can occur. When the repair is completed, the following procedure can be executed to accomplish failback to the now available primary host.

Switchover from Backup Host to Primary Host

1 When ready, log in to the backup host (e.g., for Ingest, **e0icg02**, **g0icg02**, **l0icg01**); log in as **root**.

2 On the backup host, stop all ECS functions and shut down all ECS code [refer to the procedure **Shutdown an Application** (Document 611-CD-510-001, Section 7.3.3)]. Then kill the **Subagent** on the backup.

3 Execute the failback script on the backup host (e.g., to execute the failback script on the Ingest backup, type **/failover/scripts/failback_to_icg01** and then press the **Return/Enter** key).

- The script execution relinquishes control of shared filesystems.
- ***Note***: For maximum efficiency, do not wait for completion of a step before proceeding; proceed immediately to the next steps unless the procedure directs otherwise.

4 Initiate clearing of the ARP cache in the Ebnet router by calling the Communications Manager (e.g., at GSFC, call 301-286-6141), with the request (an appropriate request for Ingest is: *"This is* <name>, <position title> *at ECS and we are going back to our primary Ingest host; to support this, we need the IPNOC to clear the ARP cache in router* <router name>. *Please advise us when this has been accomplished. My phone number is* <phone number>. *My pager number (if any) is* <pager number>.*"*

- ***Note***: Router name is **er32-1** (GSFC), **larc-gw1** (LaRC), or **edc-gw1** (EDC).

5 Initiate clearing of the ARP table in the PowerHub 8000 by calling the on-duty network administrator with the request.

- The network administrator will log in to the router as **root**, enter the <***password***>, then enter **ip arp clear**, and finally enter **bye**.

6 Log in as **root** to the primary host (e.g., for Ingest, **e0icg01**, **g0icg01**, **l0icg01**).

7 Execute the script for the primary host to resume control (e.g., for Ingest, type **/failover/scripts/resume_prime.icg**).

- The script execution gives RAID control to the primary host.

8 Log in as **root** to the MSS File Server host (e.g., **e0mss01**, **g0mss10**, **l0mss10**).

9 Execute the appropriate failback script on the MSS File Server (e.g., to execute the failback script for Ingest, type **/tools/admin/scripts/Failback_to_<*x*>icg01_CDS.csh** and then press the **Return/Enter** key).

- The script execution cleans up the CDS entries.

10 **For failover of SGI hosts attached to the HiPPI network** (otherwise, go to Step 11), execute the HiPPI switchover as follows (***Note***: EDC is the only DAAC that currently uses the HiPPI connection with Ingest):

- Log in to the secondary host as **root** and re-configure its HiPPI interface to its own IP address by executing the command **ifconfig hip0 inet <*ip address*>**.
  - ***Note***: ***ip address*** is the site- and host-unique IP address for the secondary host; refer to Appendix A of *ECS Failover Design*, Document 920-xx-xxx-xxx for the IP address needed for the specific site and host/subsystem.
- Log in to the primary host as **root** and enable the HiPPI interface by executing the command **hipcntl hip0 accept**.
- Log in to the HiPPI switch (telnet or connected terminal).
- Become **"system"** user.
- Execute command **set huntgroup <n_1> <n_2>**.
  - ***Note***: n_1 and n_2 are numbers unique to ECS sites and hosts; refer to Appendix A of *ECS Failover Design*, Document 920-xx-xxx-xxx for the numbers needed for the specific site and host/subsystem.
- Execute command **save h**.
- Log off HiPPI switch.

11 Before proceeding to Step 12, verify successful hardware switchover, as follows:

- Verify that the completion message was issued at the end of Step 7.
- To verify that the L0_buffer and data2 file systems were successfully mounted on the primary host, on that host type **df -kl** and then press the **Return/Enter** key; the returned display should be similar to the following.

```
Filesystem          Type    kbytes      use       avail     %use  Mounted on
/dev/root           xfs     3913496     2344612   1568884   60    /
/dev/dsk/xlv/buffer xfs     137775872   74247840  63528032  54    /L0_buffer
/dev/dsk/xlv/data2  xfs     4097740     2557500   1540240   63    /data2
/dev/dsk/xlv/data   xfs     8950996     1628004   7322992   19    /data1
```

- To verify that the l0buffer is exported, on the primary host enter the command **exportfs**: the returned display should be similar to the following:

```
/L0_buffer/OPS/icl
/L0_buffer/TS1/icl
/L0_buffer/TS2/icl
```

- Verify that Sybase is running on the primary host. (e.g., have the Database Administrator type isql -U<username> -P<password> -S<servername_srvr> and verify that prompt >1 appears; type quit to exit).
- Verify the ability to log in to the virtual host from another platform (e.g., from remote platform, use the ssh <x>vicgaa.<daac>b.ecs.nasa.gov command and log in to the virtual host).
- To verify that swap space is available on the new primary, type swap -ln and then press the **Return/Enter** key; the return should be similar to the following:

```
# path                    pri     pswap     free    maxswap      vswap
 2 /dev/dsk/dks1d3s1      3       2.10g     2.06g   2.10g        0.00k
 1 /dev/swap              0       512.00m   2.56m   512.00m      0.00k
g0icg01{pvan}[2]->
```

12 With hardware failback to the primary host now completed, start the Subagent (i.e., enter the command **/usr/ecs/SHARED/CUSTOM/utilities/EcMsAgStartSubagent SHARED**) and, if desired, use HP OpenView to start ECS Custom code on the host [refer to the procedure **Start an Application/Program** (Document 611-CD-510-001, Section 7.3.2)].

Performing Preventive Maintenance

There are few ECS hardware items that may require scheduled preventive maintenance. Notable items are the E-Systems Modular Automated Storage Systems (EMASS) robot, the StorageTek (STK) robot, and associated tape drives. Other items that may require periodic maintenance are the stackers and drives used for media distribution, and printers.

- Scheduled by the local Maintenance Coordinator.
- Coordinated with maintenance organization and using organization.
  - Scheduled to be performed by maintenance organization and to coincide with any corrective maintenance if possible.
  - Scheduled to minimize operational impact.
- Documented using ILM maintenance record.
  - Use *Preventative Maintenance* items screen to designate which items in the EIN file should have regularly scheduled maintenance.
  - Use *Generate PM Orders* screen to generate work orders for items needing preventive maintenance.

Analysis/Troubleshooting: COTS Software

The maintenance of COTS software items in ECS requires the management of software maintenance contracts with software vendors. This element includes:

- maintaining software use licenses.
- obtaining telephone assistance in resolving COTS software problems.
- obtaining software patches.
- obtaining software upgrades.

COTS software vendor support is contracted by the ECS procurement office at the ECS Development Facility (EDF).

- First year is under warranty support.
- Subsequent support is acquired through contract extension/modification as needed.
- COTS software support contracts data are maintained in a database used by the ECS Integrated Logistic Support (ILS) office to monitor and track contract expiration dates and terms.
- Local Maintenance Coordinators (LMC) can request changes to COTS software support contracts by contacting ILS Support.
  - Contact by e-mail can be made by using **ilsmaint@eos.hitc.com** as the address.
  - Phone contact can be made using the number 1-800-ECS-DATA (1-800-327-3282), selecting Option #3 and entering 0726 as the extension.

COTS Software Licenses

Licenses to use COTS software vary by the type of software and the software vendors' policies. License types include:

- per seat.
- per site.
- specific number of concurrent users.
- unlimited users.
- lifetime use without regard to number of users or location.

COTS software licenses are maintained in a property database. The ECS Property Administrator:

- maintains the master copy of COTS software license agreements.
- maintains the COTS software license database.
- distributes COTS software for installation at the DAACs.

The ECS Program reflects several different license restrictions based on the license types negotiated for the different COTS software products used. In general, the license restrictions are imposed through a software program that runs on a license server at the DAAC. It tracks the instances of a program in use, and when the limit is reached, it precludes access by additional operators until use falls below the limit. Table 2 lists four of the major COTS packages and identifies the license restrictions that apply to each.

Table 2. Major COTS Software License Restrictions

Software	Restriction
HP Open View	One site license, unlimited users
AutoSys	Only 1 instance at a time may be active
ClearCase®	5 users concurrently
DDTS	Virtually unlimited (10,000 users)

Installing COTS Software

The approval of appropriate CCBs is required prior to the loading of COTS software upgrades or other packages on any ECS platform. The approval process requires systematic Configuration Management (CM) procedures and documentation to ensure appropriate control of the ECS baseline and of changes to the baseline. Once the approval is received, the site Local Maintenance Coordinator notifies those personnel who will accomplish the installation (e.g., Release Installation Team, System Administrator, Network Administrator, Software Maintenance Engineer).

For ECS, there is one major tool used to facilitate CM control of software installation:

- **ClearCase**® – Provides a mountable file system that is used to store version-controlled data, such as source files, binary files, object libraries and spreadsheets.

The ClearCase® tool is used primarily for the ECS Science Software Integration and Test (SSI&T) function, but it is also applied to control changes in custom software and customized portions of some COTS software packages (e.g., configuration files).

At the DAAC, the COTS software installation actions are executed by the DAAC Software Maintenance Engineer and the System Administrator, with support as needed from ECS Development. Installation proceeds systematically. The installation is generally straightforward:

- the COTS software is installed with any ECS customization (e.g., configuration files).
- the Version Description Document (VDD) gets final updates for system and center-specific material identified by ESDIS or the operational centers, and the final VDD is available.

Safeguarding COTS Software Media

Any residual COTS software media and commercial documentation should be protected by appropriate means. For example, it may be desirable to store them in locked cabinets provided for the purpose at the DAAC. Should there be a need for access to these materials (e.g., a requirement to reload a COTS software product), keys for these cabinets can be made available from the Operations Coordinator during operating hours.

Obtaining COTS Software Support

Support of COTS software involves both site capability and contracted support. Site support is provided by the System Administrator and the Software Maintenance Engineer. When site support personnel confirm that a problem is attributable to the COTS software, the COTS Software vendor's technical support center/help desk is contacted by authorized personnel at the site. When a system problem is discovered, there is an initial troubleshooting/diagnostics procedure to be followed which is generic – i.e., not limited to software problems. However, when a software problem is indicated, the procedure refers the problem to the Maintenance Coordinator for software corrective maintenance. System troubleshooting tools and principles apply:

- Software package event browser (e.g., HP OpenView Event Browser) for sequence of events.
- Initial troubleshooting.
  - Review error message against software operator manual; prepare trouble ticket.
  - Review system logs for evidence of previous problems.
  - Attempt software reload.

  - If problem is software (e.g., hardware has been working and reload does not correct the problem), report it to the Maintenance Coordinator – i.e., forward the trouble ticket.

A problem that is not resolved through initial troubleshooting will often require troubleshooting teamwork by the Maintenance Coordinator, the System Administrator, and perhaps a Network Analyst. These troubleshooters may perform additional steps to resolve the problem:

- specific troubleshooting procedures described in COTS software manuals.
- review of the software vendor's web site's solutions database to learn of any solutions for similar problems.
- exercise any embedded or down-loadable software diagnostic routine that will determine the status of the COTS software on the equipment.
- exercise of any locally devised troubleshooting/diagnostic procedures.
- non-replacement intervention (e.g., adjustment of thresholds or other tunable parameters).

If the software problem is not resolved by the actions of the local staff, it may be necessary to request assistance through the Maintenance Coordinator from a maintenance contractor for on-site software support. Suppose, for example, that you are a Maintenance Coordinator and the site Software Maintenance Engineer has determined there is a problem with one of the COTS software packages used for Configuration Management, that initial troubleshooting finds the problem unable to be corrected locally, that a trouble ticket has been forwarded to you, and that you and System Administrator are not able to resolve the problem through additional troubleshooting. The correct approach is:

- Organize the data on the problem, find data on the appropriate support provider, and update the trouble ticket with this information.
  - Locate information such as software vendor technical support center/help desk telephone numbers, names of personnel authorized (by site and software) to contact the vendor, and the authorization/access codes available to the site's Local Maintenance Coordinator from the ECS ILS office.
- Contact the support provider's technical support center/help desk to obtain on-site assistance.
  - Provide them with the background data.
  - Obtain a case reference number from them.
  - Update the trouble ticket to reflect the time and date of the call and the case number.
  - Notify the originator of the problem that the contractor has been alerted to the problem.

- Maintain coordination with the vendor for the solution and ensure compliance with Configuration Management requirements.
    - Software vendor's technical support center/help desk verifies contract support authorization and assists in pinpointing the COTS software problem to provide a recommended solution.
    - Solution may include a patch, a work-around, or a fix in a future release of the software.
    - Assist in problem resolution (If a patch exists to correct the problem, the patch will be identified and provided by the software vendor over the Internet or mailed to the requester. If a patch is required but not available, the requester and the vendor together determine the seriousness of the problem. If the problem is critical, a temporary patch or work-around may be provided, with permanent solution to be implemented in a future update or release.).
    - The DAAC and Project Configuration Control Boards (CCBs) must authorize the patch to be installed as a permanent solution. This decision may be made after the fact, in accordance with emergency procedures required to continue to operate.
- Update trouble ticket with actions taken to correct the problem and delay time experienced for the solution, including reasons for each delay.

In preparation to request software support from the software vendor to resolve the problem, use the following procedure to obtain the background information needed.

Obtaining On-Site Software Support: Background Information

1 Collect information needed to obtain contract maintenance support.

- Obtain **version**, **release**, **serial number**, and **location** of the failed software from the software database.
- Obtain description of problem and symptoms from **trouble ticket**.
- Identify the **criticality** of the COTS software experiencing the problem.

2 Locate information on the software support vendor.

- Obtain **name**, and **telephone number** of the software support vendor.
- Obtain **access code** needed to obtain support.
- Obtain **telephone number** of the software support vendor's technical support center.
- Obtain **name** of site authorized contact person.

3 Record data on maintenance needed and maintenance provider into the trouble ticket.

In unusual cases, it may be necessary to resort to non-standard software support procedures. In the event that the software support vendor's technical support center/help desk is not providing timely successful solutions, or if the maintenance action is otherwise unsatisfactory, it may be necessary to escalate the problem to the ECS System Operations Support (SOS) group in M&O or to the Sustaining Engineering Organization (SEO). These organizations are staffed with senior systems engineers knowledgeable on COTS software and can assist with diagnosing the problem. The site Local Maintenance Coordinator may go directly to the software vendor or to the ILS Logistics Engineer to obtain an escalation of software vendor support, resulting in increased vendor management review of the problem resolution, the assignment of additional resources to resolve the problem, and/or a more highly qualified technician assigned to resolve the software problem.

This page intentionally left blank.

Troubleshooting of Custom Software

During operations, master copies of the custom software code are maintained at the ECS Development Facility (EDF). However, there may be a need to change the baseline configuration established at a given site. Changes can be driven from many sources, including the M&O organization. When changes are approved, the M&O organization performs the modification.

- Software Change Manager, ClearCase®, provides the vehicle to store and maintain the local library.
- Governing policies and minimum developed software component level that may be removed from (checked out for maintenance) or reintroduced to the master library are defined by the developers' determination of code modules.
- Configuration Management (CM) requirements apply (e.g., for configuration identification, configuration change control, and configuration status accounting).

Maintenance changes to the ECS baseline may come from any of several sources, such as:

- Changes directed by the M&O CCB.
- Site-level CCB-directed changes to configuration items, subject to ESDIS delegation of responsibility for site-level control (e.g., science software).
- Developer modifications or upgrades.
- User- or operator-initiated trouble tickets.

Implementation of Modifications

A controlled build procedure provides structure for the implementation of changes.

- Each ECS organization selects a responsible engineer (RE) for each build.
- The SOS RE establishes the set of CCRs to be included in the system build.
- Site/center REs determine applicability of any site-unique extensions for the build.
- System and center REs establish schedules for implementation, integration, and test.
- The SOS RE maintains the integrated system- and center-specific CCR list and schedule.
- The SOS RE maintains the VDD, updating it with authorized changes. Center REs provide appendices as needed to describe any center-unique additions/modifications to the build.
- The RE (or designated team) for a CCR uses the configuration-controlled library at EDF to obtain the correct version of the source code/files. The RE/team implements the change, performs programmer testing, and updates the documentation (design, interface, and procedures documents).

Obtaining Custom Software Support

The maintenance of science software and data items provided by the Science Computing Facilities (SCFs) is not the responsibility of the ECS on-site maintenance engineers. Problem resolutions and changes to this software will be handled under the auspices of local DAAC CM activities and the ESDIS CCB in the same manner as new releases to baselined science software.

Problems with ECS custom software are one type of impetus for generating trouble tickets (TTs):

- Anomalies.
- Apparent incorrect execution by an ECS software configuration item.
- Inefficiencies.
- Sub-optimal use of system resources.
- TTs may be submitted by users, operators, customers, analysts, maintenance personnel, and management staff.
- TTs capture supporting information and data related to the problem.

Troubleshooting is conducted on an ad hoc basis. Just as with COTS software problems, however, it is conducted systematically.

- Site-level activity is initiated by the Operations Supervisor assigning a trouble ticket to the Problem Investigator.
- Problem Investigator uses list of Responsible Engineers if needed to obtain support from SOS/SEO Maintenance Programmers, Responsible Engineers, and ECS Developers at the ECS Development Facility (EDF).
- EDF has the same software and computer equipment variants available at the sites, and may be able to duplicate anomalies experienced in an on-site system to derive effective resolutions or work-arounds as required until a permanent solution can be implemented.
- At a TT telecon, a priority is assigned to the TT and the TT is assigned to an organization for work-off. The organization assigns a Responsible Engineer to work off the TT. Using the data captured in the TT, the Responsible Engineer conducts a technical investigation to attempt to isolate the source of the reported problem.
- If the problem is caused by a non-ECS element (e.g., an interface problem with an external system, poor resource usage by a science algorithm, poor performance by a non-ECS service), the TT and supporting data are provided to the maintainer of that element. An ECS CCR may also be proposed to protect ECS from potential threats of future problems identical or similar to that documented in the TT.

General ECS Troubleshooting

The troubleshooting approach presented here is derived in part from procedures applicable during system installation and general checkout, but it also includes procedures applicable for analyzing

symptoms or problems encountered in specific operations involving specific subsystems. Many ECS problems can be traced to accessibility and communications among the multiple clients and servers on which ECS functions are so heavily dependent. Figure 13 provides a chart identifying problem categories at a top level. In the chart, each category is listed in a separate box with an associated identifying number and a reference to a numbered procedure for troubleshooting problems in that category. Figure 14 consists of a series of flow charts reflecting the numbered procedures. The numbered procedures with detailed troubleshooting steps are presented in the pages following Figure 14. If a problem presents specific symptoms suggesting a failure of a type known to be associated with a specific subsystem or a specific function (e.g., Ingest, Planning, Data Processing, Data Distribution), it may be helpful to refer to troubleshooting guidance and procedures presented in lessons addressing that subsystem or function. Otherwise, use the top-level chart in Figure 13 to locate an appropriate detailed flowchart and step-by-step procedure for troubleshooting. The detailed charts in Figure 14 depict troubleshooting flow and decisions. Exit from the flow reflects either resolution of the problem or failure to identify and resolve it. If the problem cannot be identified and resolved without help within a reasonable period of time, the appropriate response is to call the help desk and submit a trouble ticket in accordance with site and system Problem Management policy.

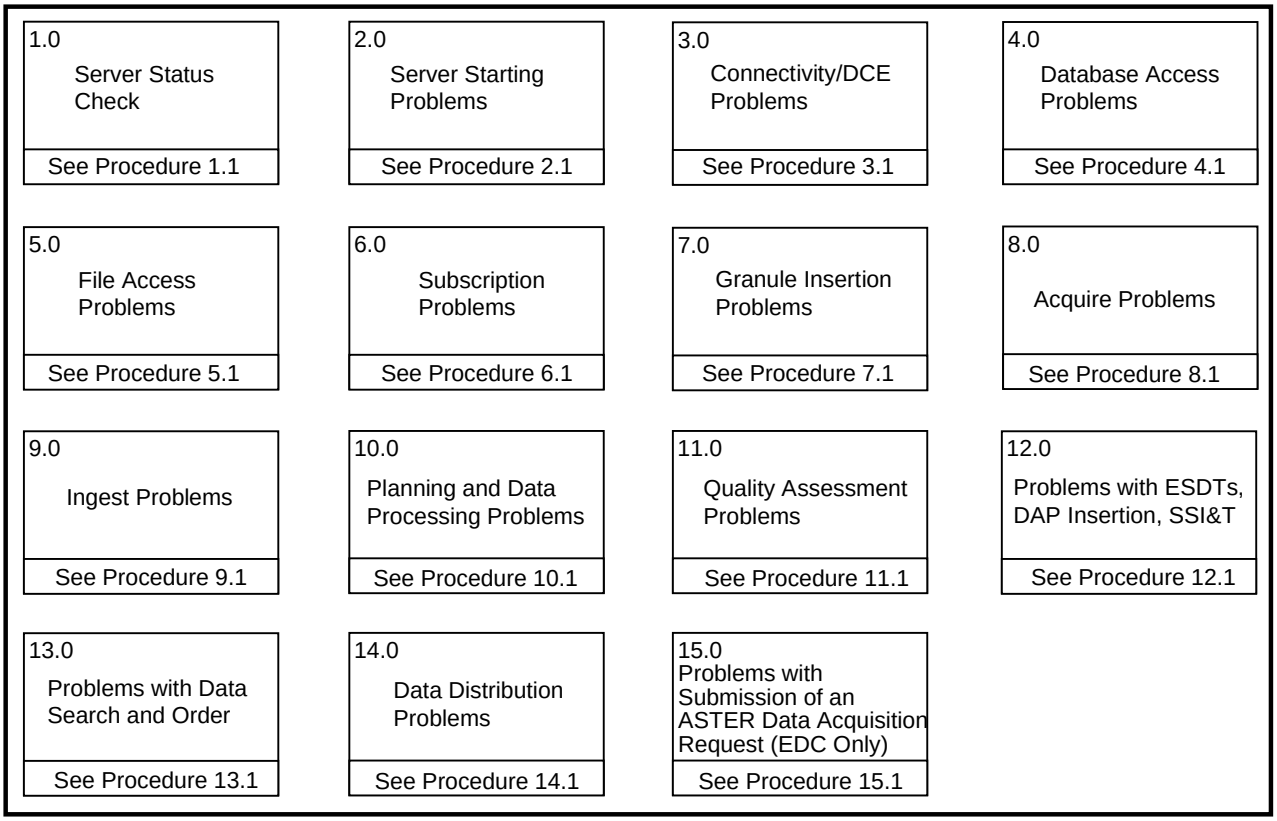


Figure 13. Top-Level Problem Categories

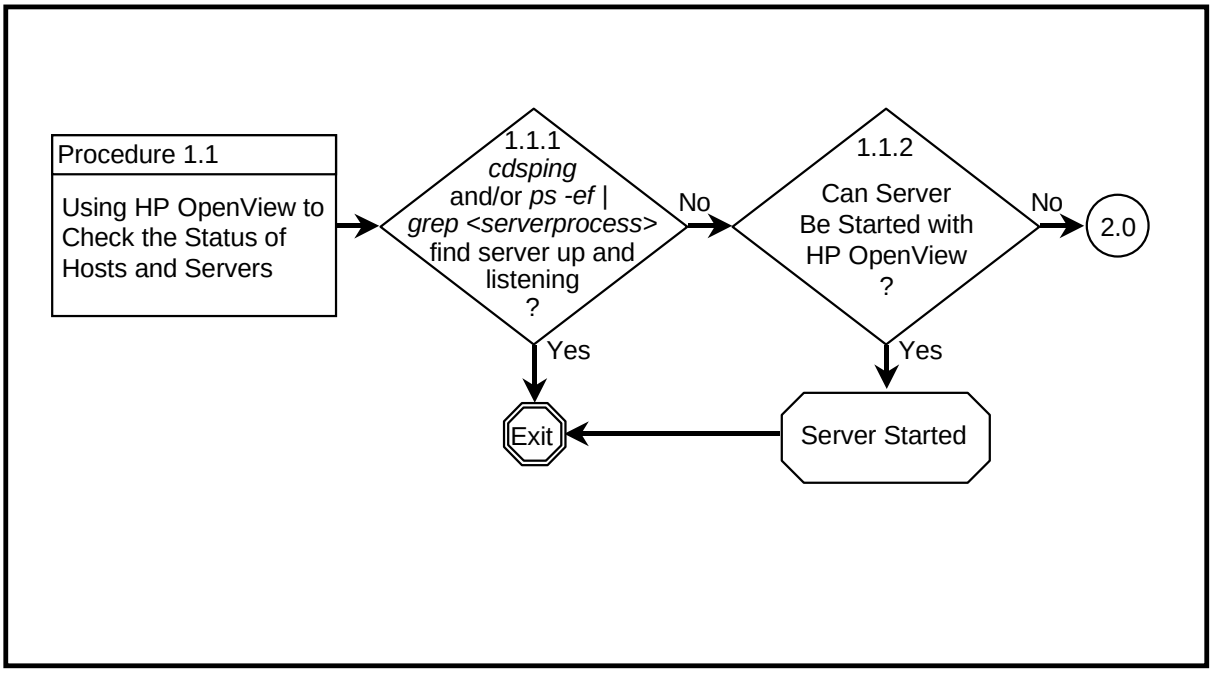


Figure 14a. 1.0: Server Status Checks

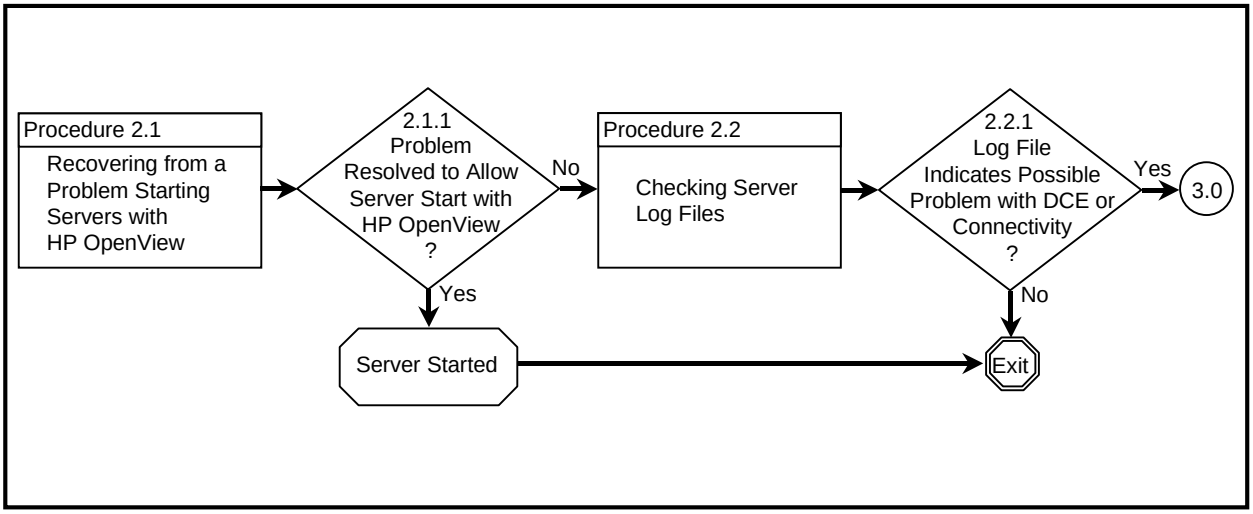


Figure 14b. 2.0: Server Starting Problems

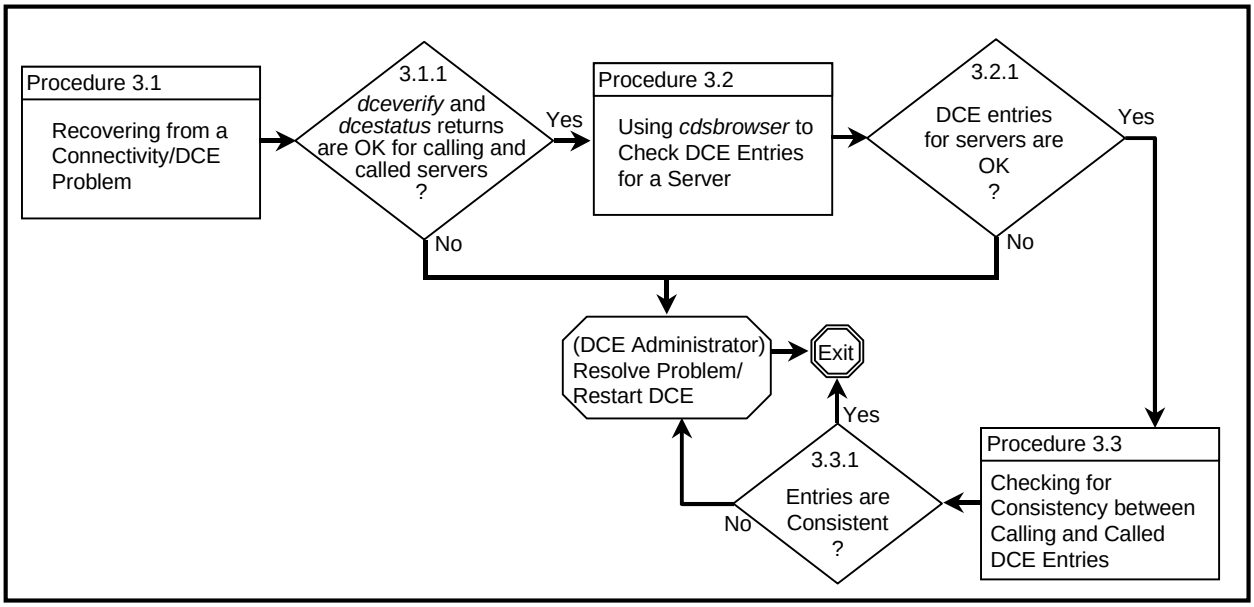


Figure 14c. 3.0: Connectivity/DCE Problems

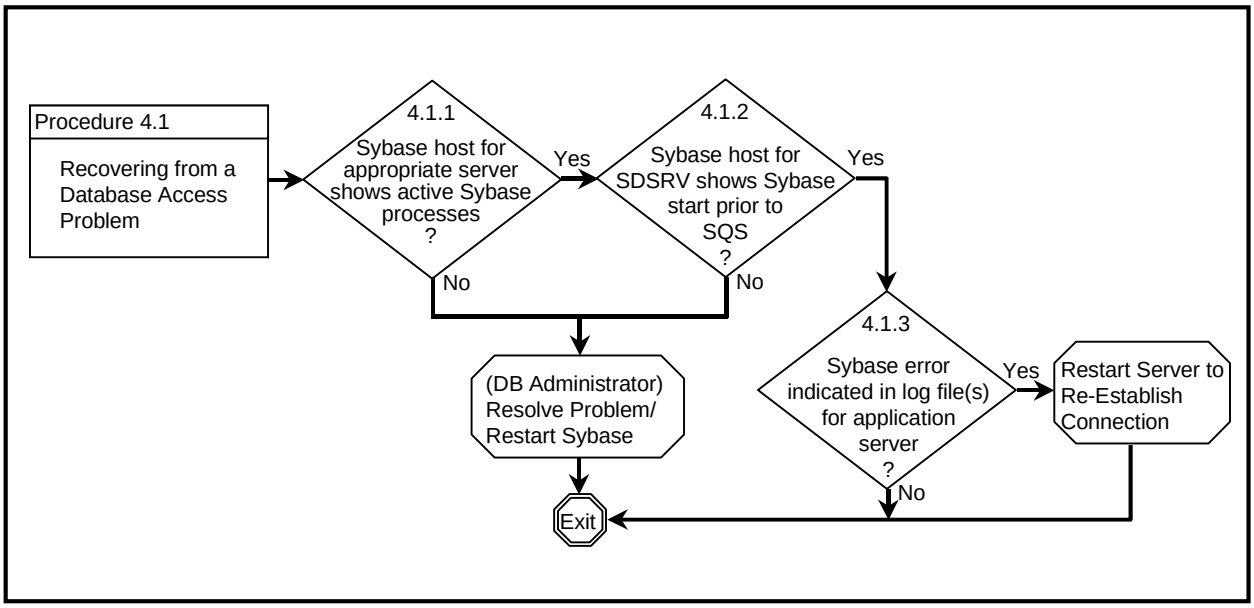


Figure 14d. 4.0: Database Access Problems

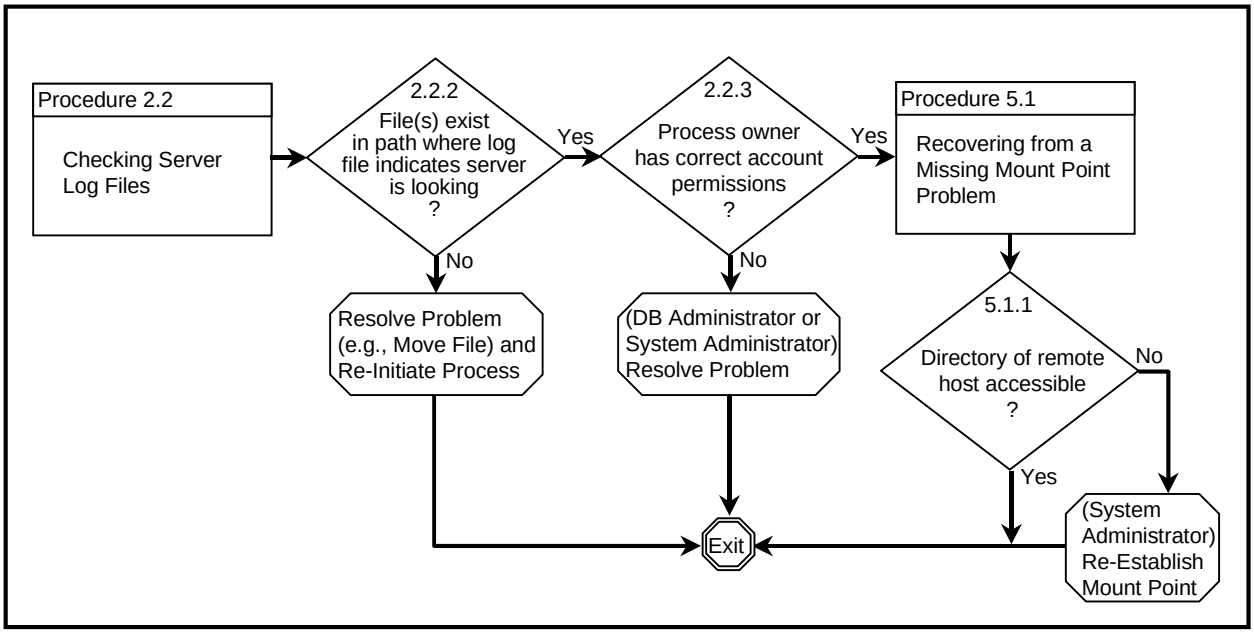


Figure 14e. 5.0: File Access Problems

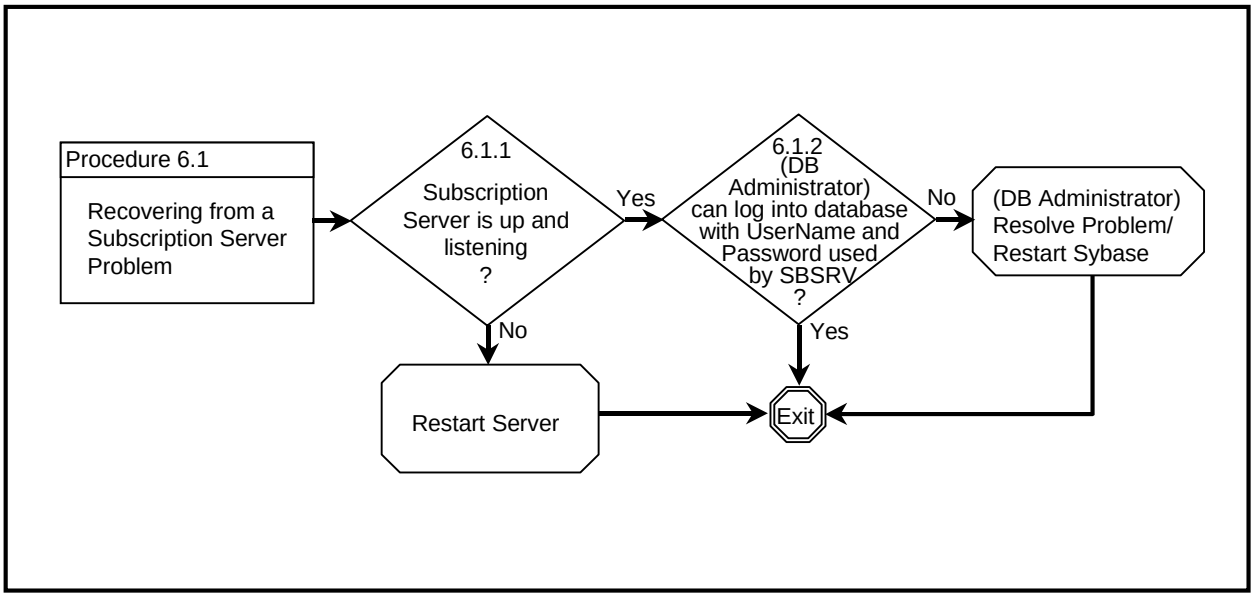


Figure 14f. 6.0: Subscription Problems

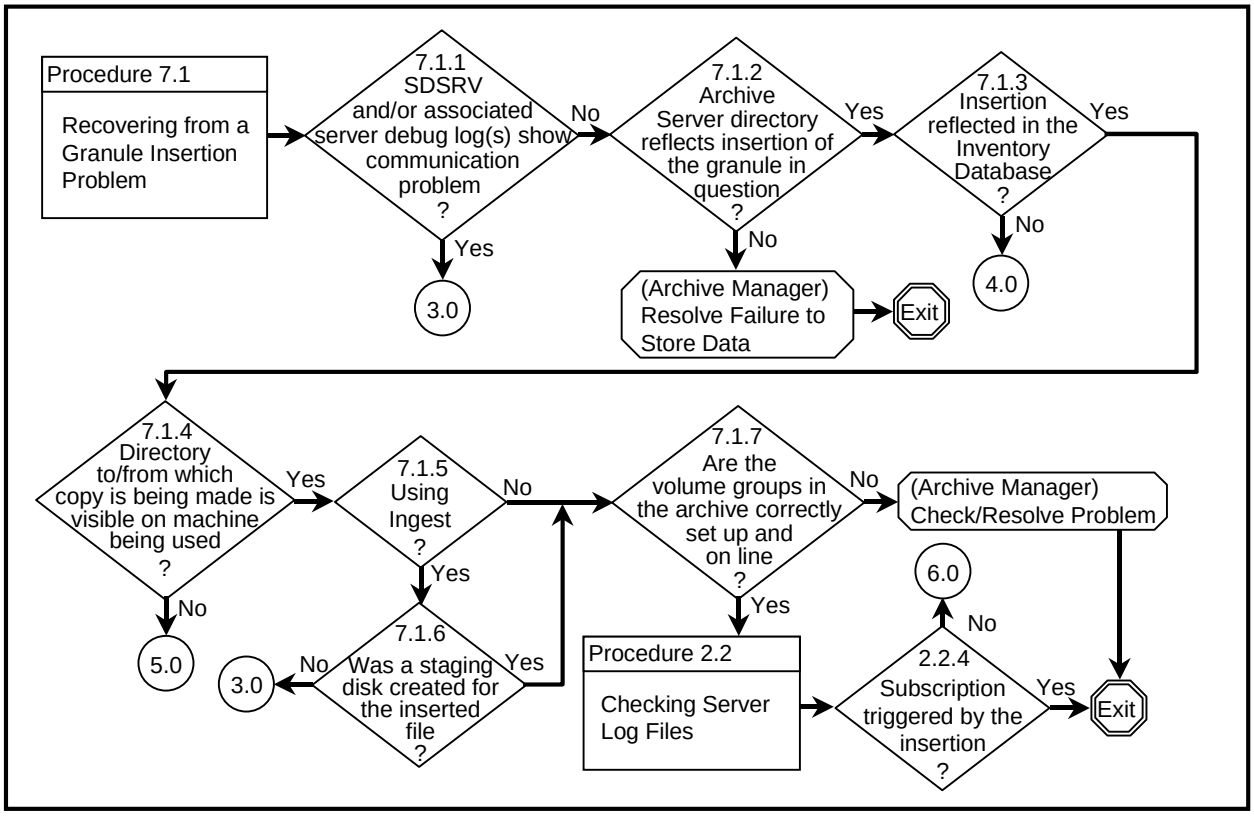


Figure 14g. 7.0: Granule Insertion Problems

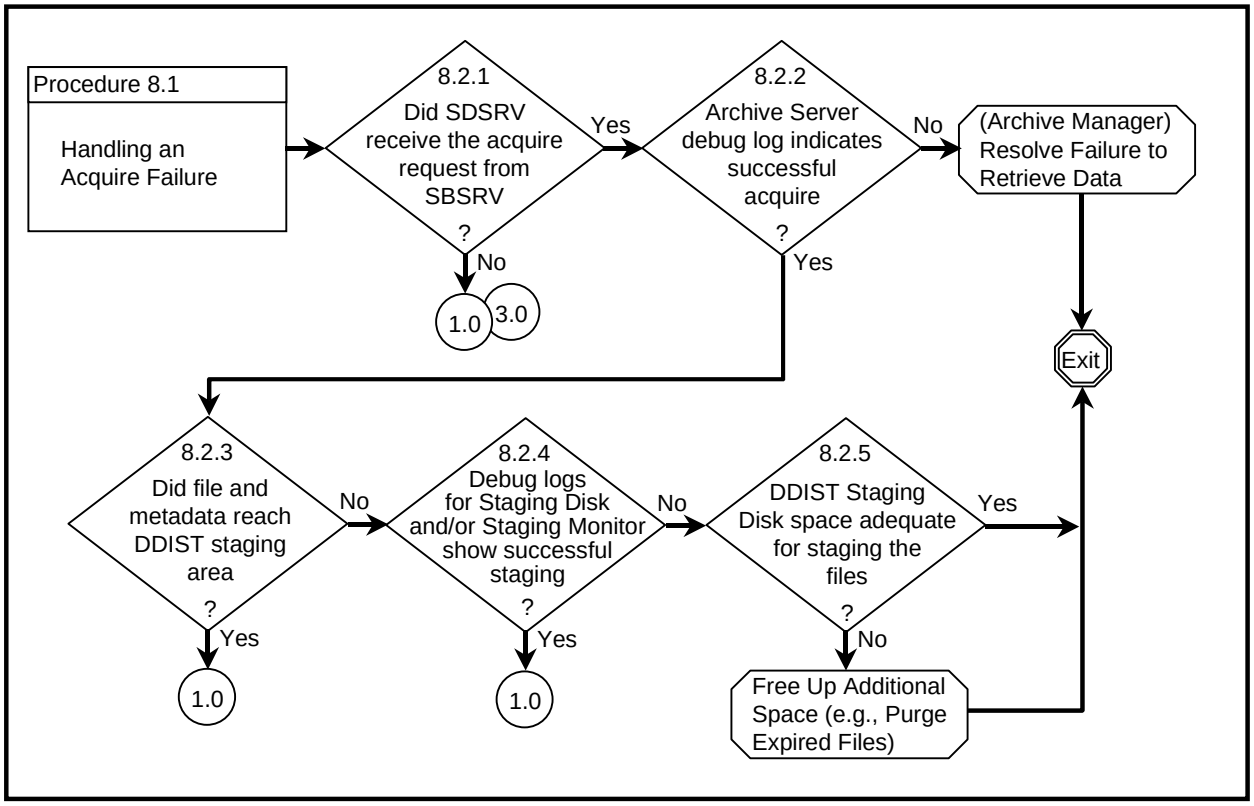


Figure 14h. 8.0: Acquire Problems

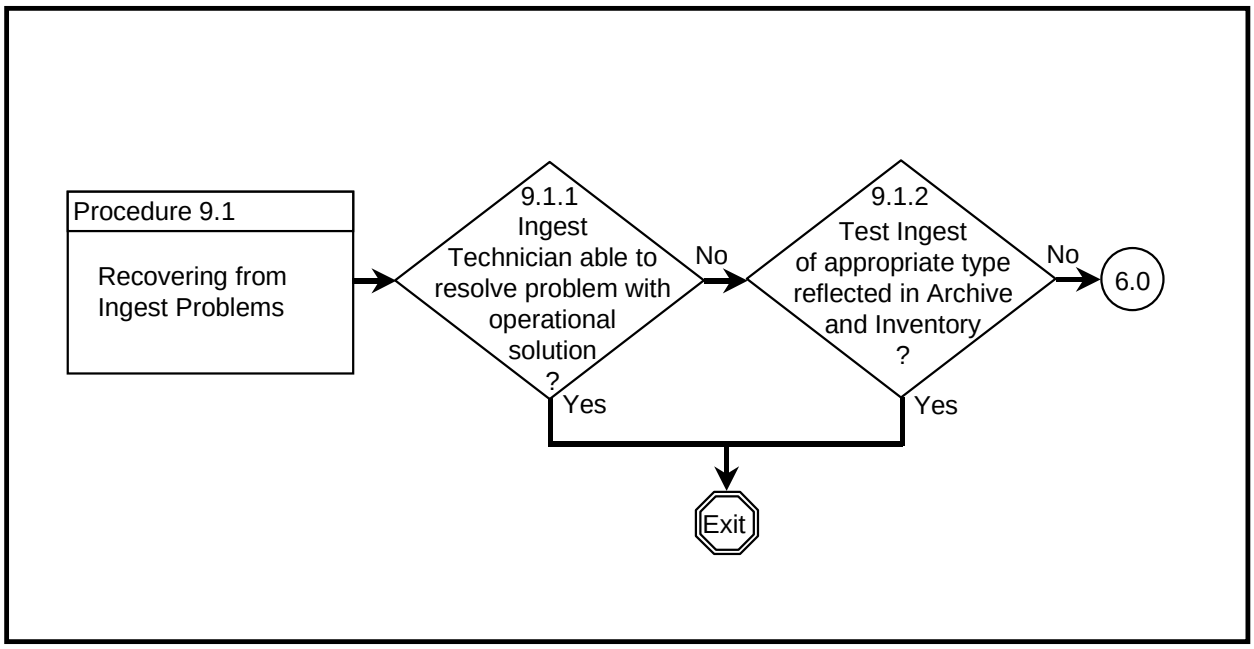


Figure 14i. 9.0: Ingest Problems

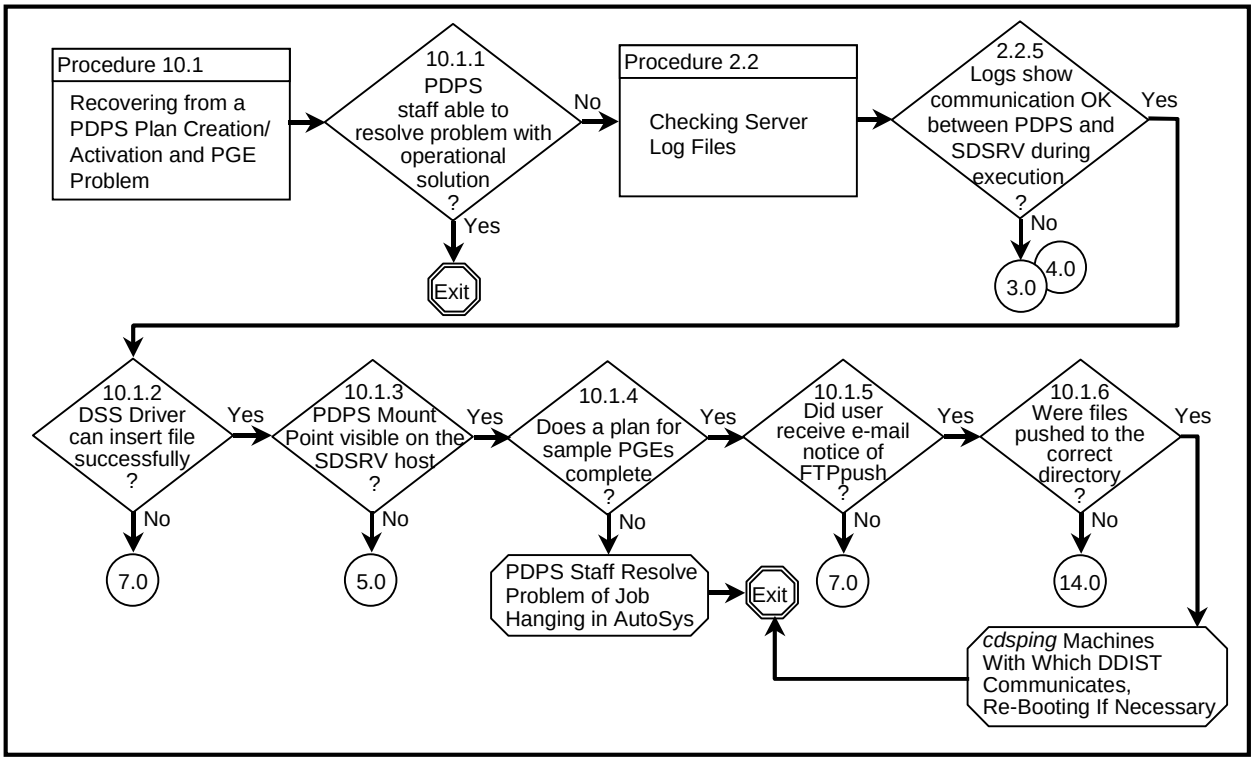


Figure 14j. 10.0: Planning and Data Processing Problems

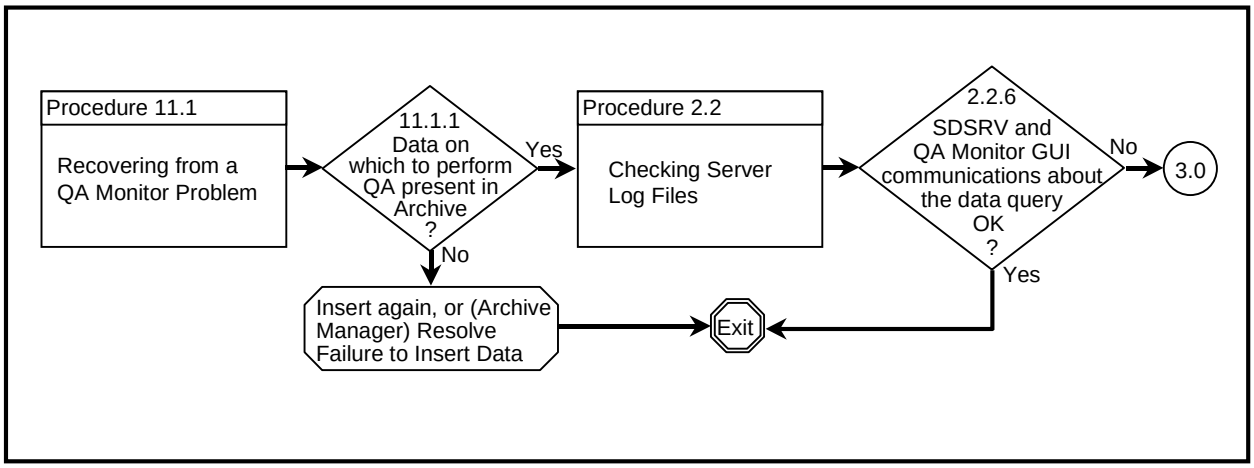


Figure 14k. 11.0: Quality Assessment Problems

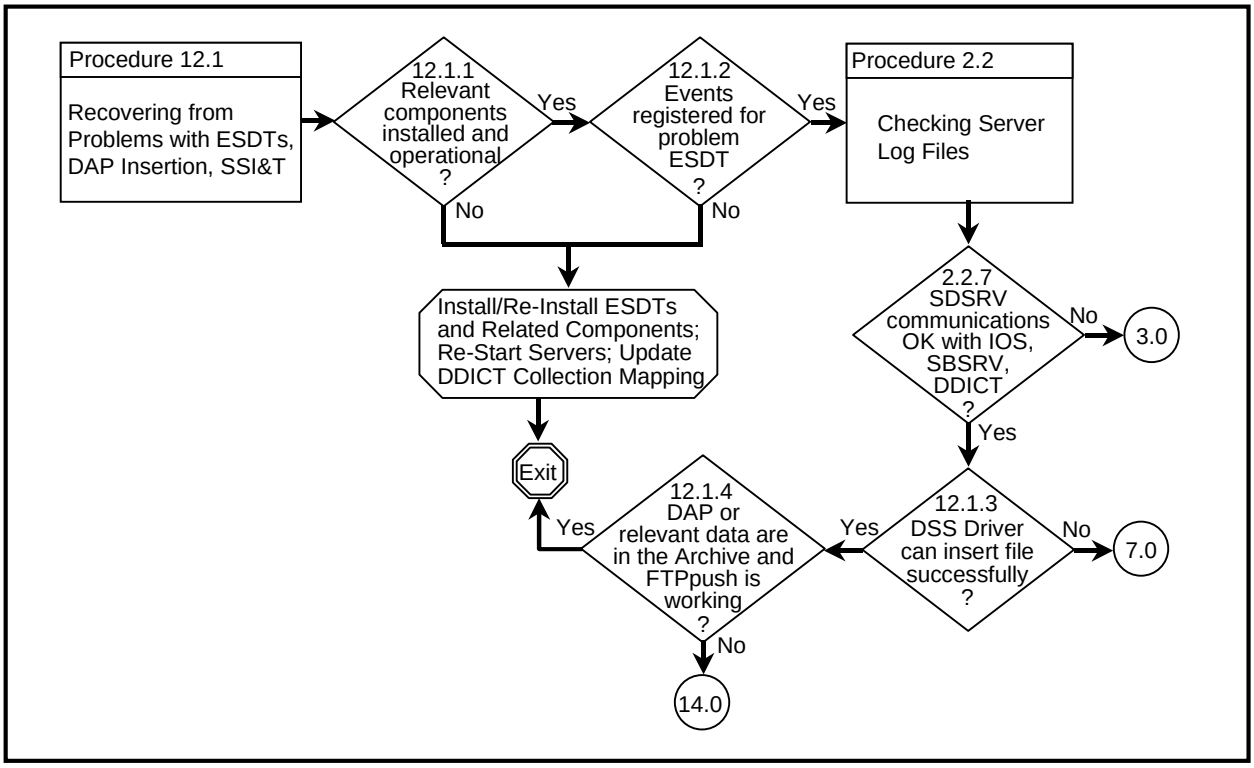


Figure 14l. 12.0: Problems with ESDTs, DAP Insertion, SSI&T

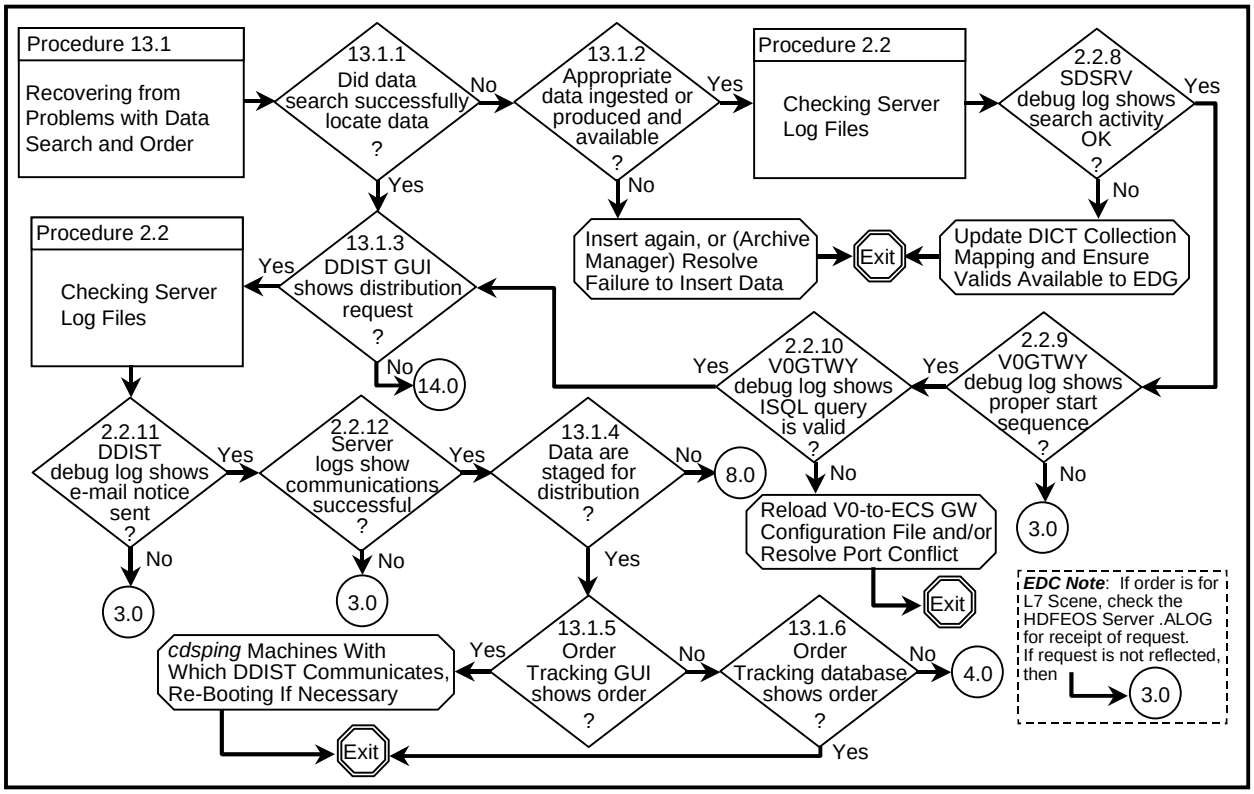


Figure 14m. 13.0: Problems with Data Search and Order

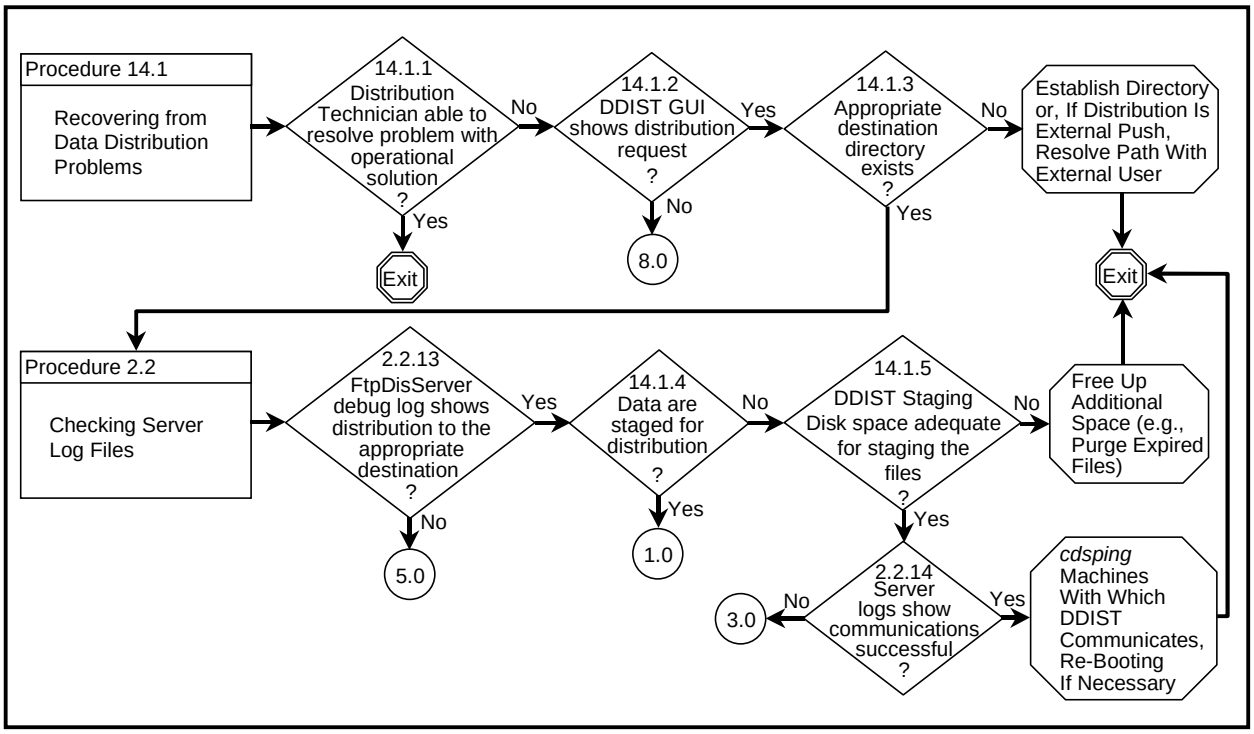


Figure 14n. 14.0: Data Distribution Problems

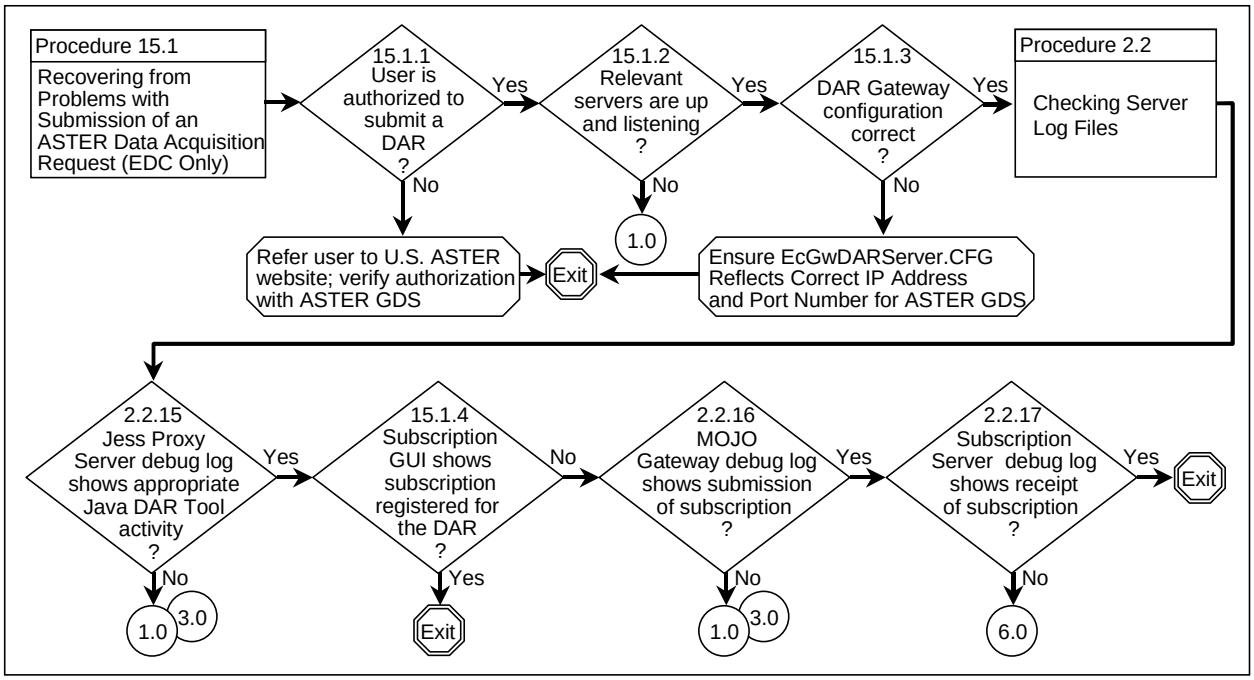


Figure 14o. 15.0: Problems with Data Acquisition Requests (EDC Only)

Using HP OpenView to Check the Status of Hosts and Servers

HP OpenView is the primary means of visually checking the status of ECS processes. It is a multi-vendor network management tool that provides system administrators with a means to start and stop ECS servers and to monitor their status. This can be accomplished either at an overall Mode level (i.e., TS1, TS2, or OPS) or individual System level (e.g., MSS, IDG).

The program's graphical user interface (GUI) presents a series of screens that enable the user to progressively dig deeper into the status of the system. Figure 15 is the initial program screen displayed after starting HP OpenView.

Figure 15. HPOV Root window

Figure 16 through Figure 20 are examples of screens the user would access by working down via the **Service** icon to display the status of a sub-system server. They include the Services submap window (Figure 16), the overall Mode submap window (Figure 17), the OPS Mode submap window (Figure 18), a zoomed-in view of the OPS Mode submap window (Figure 19), and the zoomed-in view with a child window resulting from a double-click on one of the icons (Figure 20) showing all the way down into the system to the status screen for a specific server (EcSbSubServer).

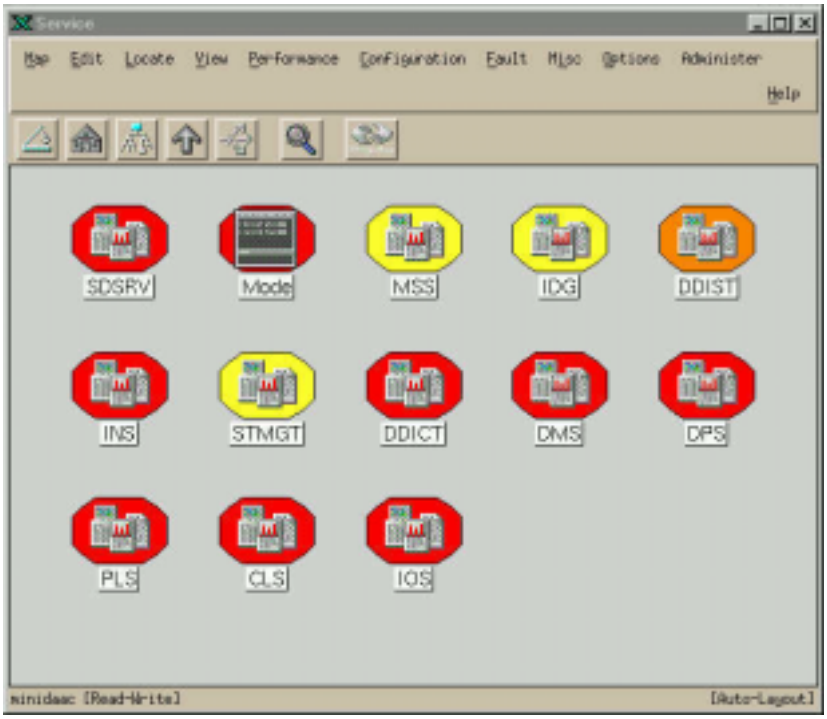


Figure 16. Service submap window

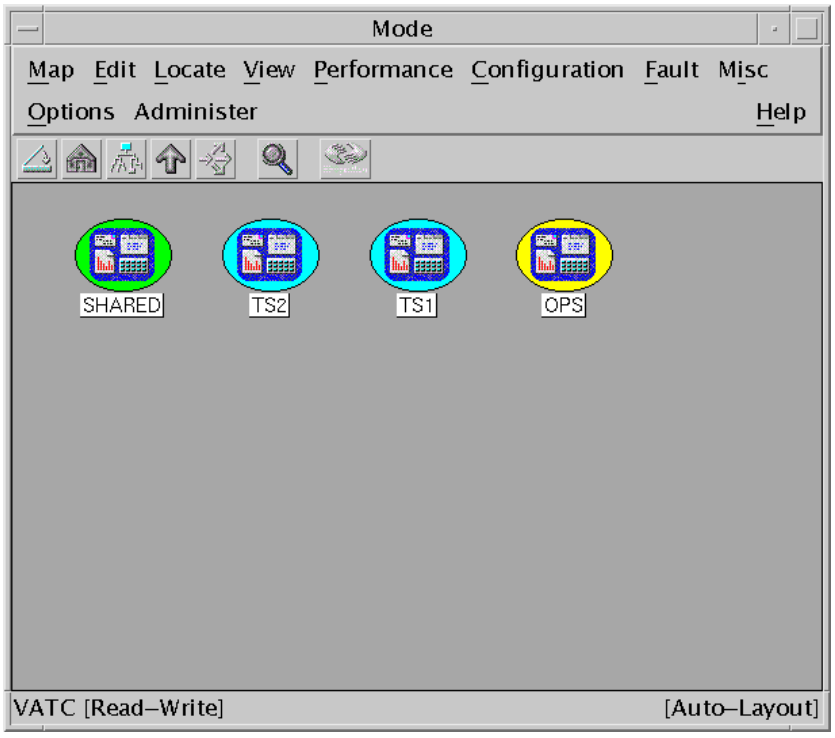


Figure 17. Mode submap window

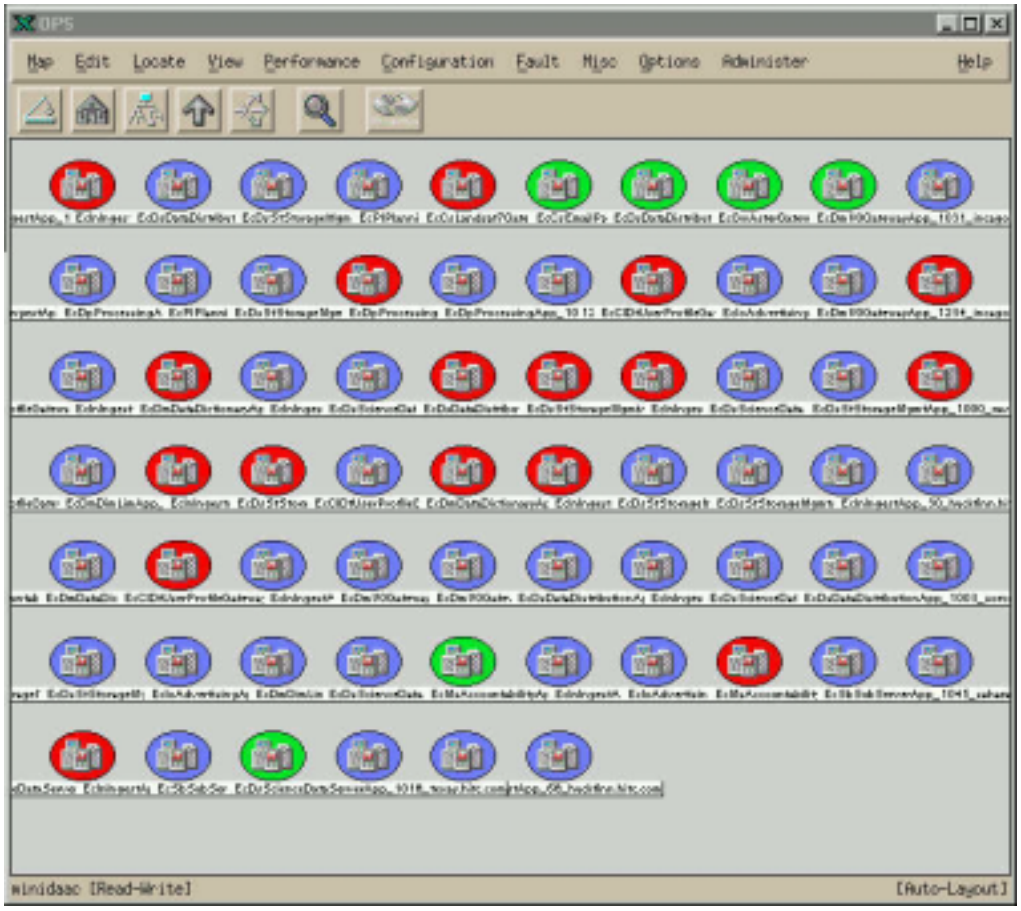


Figure 18. OPS Mode submap window

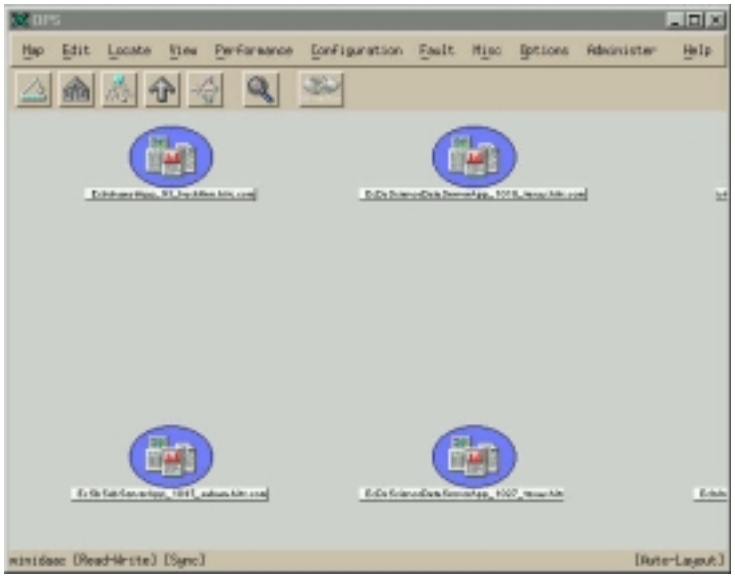


Figure 19. Zoom view of OPS submap window

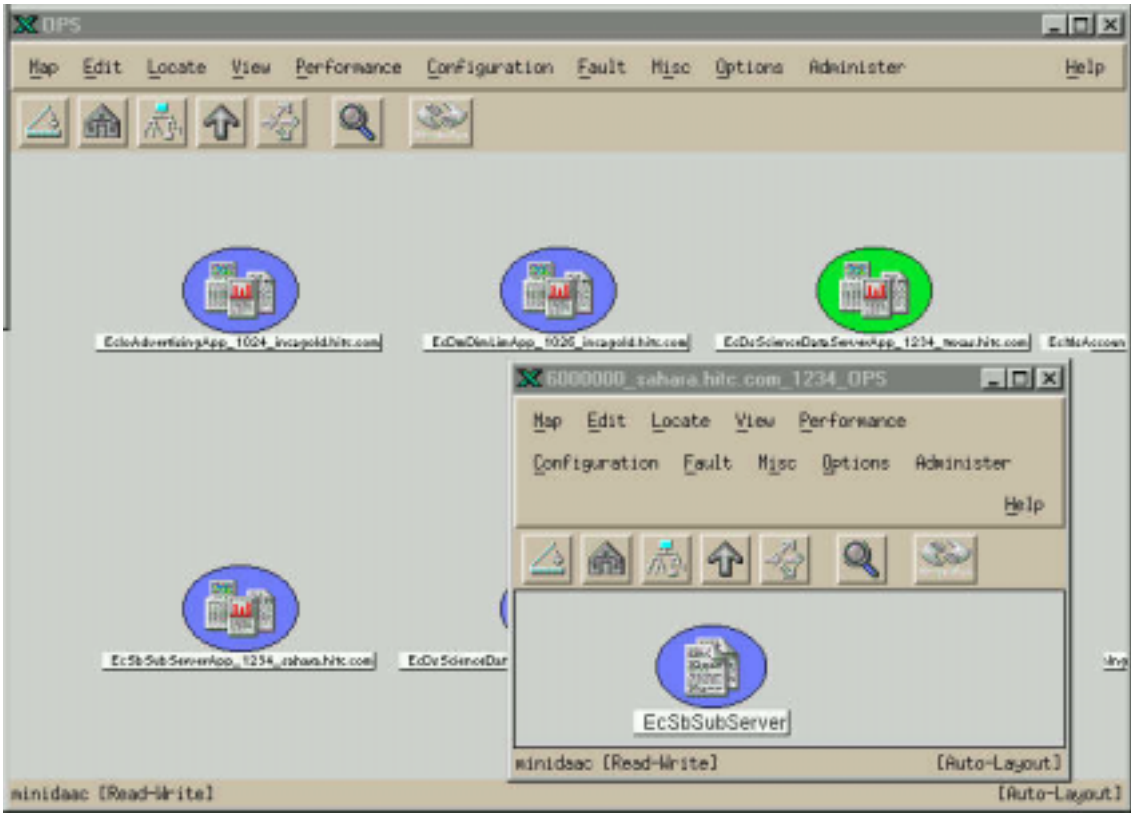


Figure 20. Server status submap

To view server status, perform the following procedure.

Using HP OpenView to Check the Status of Hosts and Servers (Procedure 1.1)

1 Log in to the *HP OpenView* host.

2 Type **/usr/ecs/<*mode*>/COTS/OV/bin/ovstatus** at a UNIX command prompt and then press the **Return/Enter** key.

- A series of messages is displayed indicating for each process that its state is "**RUNNING**" or "**NOT_RUNNING**."
- If the network management processes are not running, a system administrator (logged in as **root**) can start them by typing **/usr/ecs/<*mode*>/COTS/OV/bin/ovstart**, and then pressing the **Return/Enter** key.

3 Type **/usr/ecs/<*mode*>/COTS/OV/bin/ovw &,** and press the **Return/Enter** key.

- The **About OVW** box is displayed, followed in a few moments by the OVW Root window and any installed and registered NNM applications are also started.

4 Double click on the **Service** icon.

- The **Service** submap is displayed.

5 From the **Service** submap, to check the status of all applications and servers for a given mode (i.e., TS1, TS2, OPS), select the **Mode** icon to bring up the **Mode** submap. To monitor applications and servers across all modes (e.g., CLS, MSS, IDG), select the icon for a specific subsystem.

- As an example, selecting **OPS** mode will display a submap showing all the applications for the OPS mode on each host.
- Using the HP OpenView Pan and Zoom function that is described in the System Administration lesson, 625-CD-004-002, will enable you to see the data under each icon more clearly.

6 At this point, select the icon for the Application you are investigating (e.g., EcSbSubServerApp) that might be indicating status information not available (blue color). Double clicking on this icon will display a window that shows the status of the actual server for which you are determining status.

7 If it is necessary to restart a server, refer to detailed instructions to **Start an Application/Program** (Document 611-CD-510-001, Section 7.3.2).

Recovering from a Problem Starting Servers with HP OpenView

Starting a server using HP OpenView requires that two processes be running on the host for HP OpenView. These are the Deputy Agent (**EcMsAgDeputy**) and the start daemon (**EcMsCmEcsd**). Furthermore, it requires that the Subagent (**EcMsAgSubAgent**) be running on the host for the server to be started. Therefore, if a server cannot be started from HP OpenView, it is necessary to ensure that these processes are running.

If these processes are running and a server still cannot be started from HP OpenView, there are two alternative choices:

- starting the server using ECS Assistant.
- starting the server from a command-line prompt.

Using ECS Assistant provides a Graphical User Interface (GUI) method to start a server with subsequent screen displays showing server status. Command-line entries require a more in-depth knowledge of the system and an understanding of the inter-relationships of various processes. Use the following procedure to recover from a problem starting servers with HP OpenView.

Recovering from a Problem Starting Servers with HP OpenView (Procedure 2.1)

1 Log into the *HP OpenView* host.

2 Verify that the HP OpenView run executables are running in **SHARED** mode.

- Type **ps -ef | grep EcMsAgDeputy**, and then press the **Return/Enter** key. The resulting display should be similar to :

. . . .
cmshared 15727 15102 0 15:52:10 ttypa 0:00 grep EcMsAgDeputy
cmshared 28274 1 0 Apr 6 ? 158:20
/usr/ecs/SHARED/CUSTOM/bin/MSS/EcMsAgDeputy ConfigFile /usr/
. . . .

- Then type **ps -ef | grep EcMsCmEcsd**, and press the **Return/Enter** key. The resulting display should be similar to:

. . . .
cmshared 28208 1 0 Apr 6 ? 101:47
/usr/ecs/SHARED/CUSTOM/bin/MSS/EcMsCmEcsd
cmshared 15798 15102 1 15:52:31 ttypa 0:00 grep EcMsCmEcsd
. . . .

- If the executables are running, go to step 6.

3 If the executables are not running, type **cd /usr/ecs/SHARED/CUSTOM/utilities** and press the **Return/Enter** key.

- The prompt will indicate a change to the **SHARED** directory, **/usr/ecs/SHARED/CUSTOM/utilities,** where the HP OpenView run executables are located.

4 Start the executables with a command-line prompt.

- Type **EcMsAgDeputyStart SHARED** and press the **Return/Enter** key.
- Then type **EcMsCmStartEcsd SHARED** and press the **Return/Enter** key.

5 Verify that the executables are running by repeating step 2.

6 Log onto the host with the server to be started.

7 Verify that the HP OpenView sub agent is running.

- Type **ps -ef | grep EcMsAgSubAgent** and press the **Return/Enter** key. The resulting display should be similar to :

. . . .
cmshared 29306 1 0 Apr 13 ? 99:00
/usr/ecs/SHARED/CUSTOM/bin/MSS/EcMsAgSubAgent ConfigFile
/usr/ecs/SHARED/CUSTOM
cmshared 16538 16413 0 15:53:56 pts/9 0:00 grep EcMsAgSubAgent
. . . .

- If the executable is running, go to step 10.

8 If the executable is not running, type **cd /usr/ecs/SHARED/CUSTOM/utilities** and press the **Return/Enter** key.

- The prompt will indicate a change to the **SHARED** directory, **/usr/ecs/SHARED/CUSTOM/utilities,** where the HP OpenView run executable is located.

9 Start the executable with a command line prompt.

- Type **EcMsAgSubAgentStart SHARED** and press the **Enter.**

10 Verify that the executable is running by repeating step 7.

11 If the executables are running and the target server fails to start using HP OpenView, use ECS Assistant to start it [refer to detailed instructions **Using ECS Assistant to Start Up/Shut Down Servers** (Document 611-CD-510-001, Section 3.7.2)].

- If the servers start, go to the procedure **Checking Server Log Files (Procedure 2.2)** and review server log files (in this case, **EcMsAgDeputyDebug.log**, and **EcMsAgSubAgentDebug.log**) for evidence of communications or DCE problems.

12 If the servers do not start, use command line entries to start the servers.

- On the host for the server to be started, type **cd /usr/ecs/<*mode*>/CUSTOM/utilities**, and press the **Return/Enter** key.
- The prompt will indicate a change to the **/usr/ecs/<*mode*>/CUSTOM/utilities/** directory, where the Application and Server startup files are located.
- Type **ls**, then press the **Return/Enter** key. The resulting display should include entries similar to the following:

. . . .

<*hostname*>{cmshared}60: ls

EcClDtUserProfileGatewayAppMkcfg	**EcDmEcsToV0GatewayStart**
EcClDtUserProfileGatewayAppStart	**EcDmEnvKsh**
EcClDtUserProfileGatewayMkcfg	**EcDmLimServerMkcfg**
EcClDtUserProfileGatewayStart	**EcDmLimServerStart**
EcCsEmailParserAppMkcfg	**EcGwAsterGatewaysAppStart**
EcCsEmailParserAppStart	**EcGwDARServerMkcfg**
EcCsEmailParserMkcfg	**EcGwDARServerStart**
EcCsEmailParserStart	**EcIoAdCGIProgsMkcfg**

. . . .

- Type **<*name*>AppStart <*mode*>** (i.e., **EcGwAsterGatewaysAppStart OPS**) and press the **Return/Enter** key to start the selected application.
- Type <***name***>**ServerStart> <*mode*>** (i.e., **EcGwDARServerStart OPS**) and press the **Return/Enter** key to start the selected server.
- Verify the server has started using HP OpenView, ECS Assistant, or the command-line check, **ping_by_name**, described in the procedure **Recovering from a Connectivity/DCE Problem (Procedure 3.1)** (subsequent section of this lesson).
- If the server has not started, it may be necessary to reinstall the server software.

Checking Server Log Files

The functioning of ECS requires communication among servers in a Distributed Computing Environment (DCE). Therefore, if system performance degradations occur, initial things to look for include DCE connection problems. Some of these may be reflected in the log files (e.g., error messages at server start up). Log files can often provide information that will identify possible sources of disruption in server function or communications, suggesting additional checks or actions that may help resolve the problem. It may be necessary to examine logs both on the server being called and on the server from which the call is made. The procedure for checking a log file starts with the assumption that the operator has logged in to ECS.

Checking Server Log Files (Procedure 2.2)

1 Log in to the host for the server and log(s) to be examined.

2 Type **cd /usr/ecs/<*MODE*>/CUSTOM/logs** and then press the **Return/Enter** key.

- The prompt reflects the change to directory **/usr/ecs/<*MODE*>/CUSTOM/logs**.

3 To view a server log, type **pg *filename*** and then press the **Return/Enter** key.

- ***filename*** refers to the log file to be reviewed (e.g., **EcMsAcRegUserSrvr.ALOG**, **EcMsAcRegUserSrvrDebug.log**).
- The first page of the log file is displayed; additional sequential pages can be displayed by pressing the **Return/Enter** key at the **:** prompt.
- Although this procedure has been written for the **pg** command, any UNIX editor or visualizing command (e.g., **vi**, **more**, **tail**) can be used to review the log file.
- Typically, the **<*server*>Debug.log** captures more detailed information than the **<*server*>.ALOG**. However, for some servers (e.g., **SDSRV**), there may be significant detail in the **<*server*>.ALOG**. It is also important to note that the **DebugLevel** setting in the **<*server*>.CFG** file determines the level of detail captured in the **<*server*>Debug.log** (**0** is off, a setting of **1** captures status and errors, a setting of **2** captures major events, and a setting of **3** is a full trace recording of all activity). If the **DebugLevel** has been set to one of the lower levels during operations, the System Administrator may set it to **3** during troubleshooting.

4 Review the log file(s) to determine if there are any indications of connection problems (DCE) or errors at start up.

- The log file for the called server may contain an error message concerning **PF Init** or some **DCE** error or problem.
- The log file for the server from which the call originated may indicate a **DCE** or other connection problem (e.g., **Binding not found in cache . . .**, **DCE error: invalid binding . . .**, **Unable to get resource . . .**).
- This procedure is applicable for reviewing logs for different types of errors and events on ECS servers.

5 Exit the log file (e.g., from **pg**, type **q** and then press the **Return/Enter** key).

6 If one or more log files indicate connection problems or DCE errors, continue with the procedure for **Recovering from a Connectivity/DCE Problem (Procedure 3.1)**.

Recovering from a Connectivity/DCE Problem

If a review of relevant log files suggests that there may be a problem with connectivity or DCE, there are several actions that may restore server and communications accessibility. Use the following procedure. The procedure starts with the assumption that the operator is logged in to ECS.

Recovering from a Connectivity/DCE Problem (Procedure 3.1)

1 Ensure the "up" status of the server(s) in question using HP OpenView to view the status of hosts and application servers, and restart any server that is down.

- Refer to specific procedures in Sections 7.1.2, 7.1.3, and 7.3 of 611-CD-510-001 *Mission Operation Procedures for the ECS Project*.

2 From the command line prompt, attempt to ping the server(s) in question by typing **ping_by_name /.:/subsys/ecs/<*mode*>/<*server*>**.

- The following type of response should be returned:

  Read CDS entry / . . . /<*cell*>/subsys/ecs/servers/<*host*>/Server/ . . .
  Binding . . . .
  Checking interfaces . . .
  interface . . . .
  Checking objects . . .
  object UUID . . . .
  Trying interface . . . .
  Attempt to resolve the endpoint . . .
  . . . .

attempt to ping . . .
SERVER RESPONDS to ping (17 ms)
checking server principal name . . .
principal /. . . /<*cell*>/<*server*>
checking statistics . . .
calls in / out: 15 / 578
packets in / out: 825 / 725

- If the server does not respond, return to Step 1.

3 Log in to the host for the called server; from the command line prompt, type **/tools/bin/dceverify** and then press the **Return/Enter** key.

- If DCE is working properly, the return should identify the host, operating system, and DCE cell, and show that the system, Daemons, security, and CDS are OK. The output should be similar to the following:

DCE Verification - v1.0

Host: <*hostname*>
OS: SunOS 5.5.1
DCE Cell: <*xxxxxx.xxxx.xxx*>
System: OK
DCE Daemons: OK
Security: OK
CDS: OK

- If the output does not verify that DCE is **OK**, it may be necessary to have DCE restarted on the server host.

4 From the command line prompt, type **/tools/bin/dcestatus** and then press the **Return/Enter** key.

- If DCE is working properly, the return should provide DCE information and status on the daemons that are running on the host. The output should be similar to the following:

*****************DCE Information***********************

Machine_type is: SunOS
The Machine Name is <*name*>
The OS Patch Level is ---> (*nn*)
The Cell Name is: /…/<*xxxxxx.xxxx.xxx*>
The Clearinghouses are:
/…/<*xxxxxx.xxxx.xxx*>/<*xxxxxxxx*>_ch
/…/<*yyyyyy.yyyy.yyy*>/<*yyyyyyyy*>_ch
*****************DCE Patch Level for SUN*****************
DCE Patch Level is Transarc DCE 1.1
Solaris 2.5
Patch <*nn*> <*date*>
US Version
Copyright <*date*> by Transarc Corp.
*****************DCE Daemons Running Are*****************

```
DCE daemons
F S UID  PID  PPID C  PRI  NI   ADDR     SZ  WCHAN TTY  TIME  CMD
n S 0    nnn  1    0  nn   20   nnnnxnnn nnn nnnnxnnn ?    n:nn  dced
n S 0    nnn  1    0  nn   20   nnnnynnn nnn nnnnynnn ?    n:nn  cdsadv
n S 0    nnn  1    0  nn   20   nnnnznnn nnn nnnnznnn ?    n:nn  dtsd
DFS daemons
F S UID  PID  PPID C  PRI  NI   ADDR     SZ  WCHAN TTY  TIME  CMD
License daemons
F S UID  PID  PPID C  PRI  NI   ADDR     SZ  WCHAN TTY  TIME  CMD
**************************************************
```

- If the output does not indicate DCE information and daemons running, it may be necessary to have DCE restarted on the server host.

5 If **dceverify** and **dcestatus** return appropriate information on the host for the called server, repeat steps 3 and 4 for the host from which the call originated.

- If necessary, have DCE restarted on the server host.

6 If **dceverify** and **dcestatus** return appropriate information on both the called and calling server host, continue with the procedure for **Using *cdsbrowser* to Check DCE Entries for a Server (Procedure 3.2)** (subsequent section of this lesson).

Using *cdsbrowser* to Check DCE Entries for a Server

Even if DCE is functioning properly on server hosts, there may be problems with DCE entries for server applications. In order for ECS to function, the calling server or client must use the correct DCE entry for the server in question. The *cdsbrowser* is a useful tool for checking DCE entries. Figure 21 shows two screens from the *cdsbrowser*. The screen on the left side of the figure is the initial screen, and the one on the right shows an example of entries associated with an ECS server.

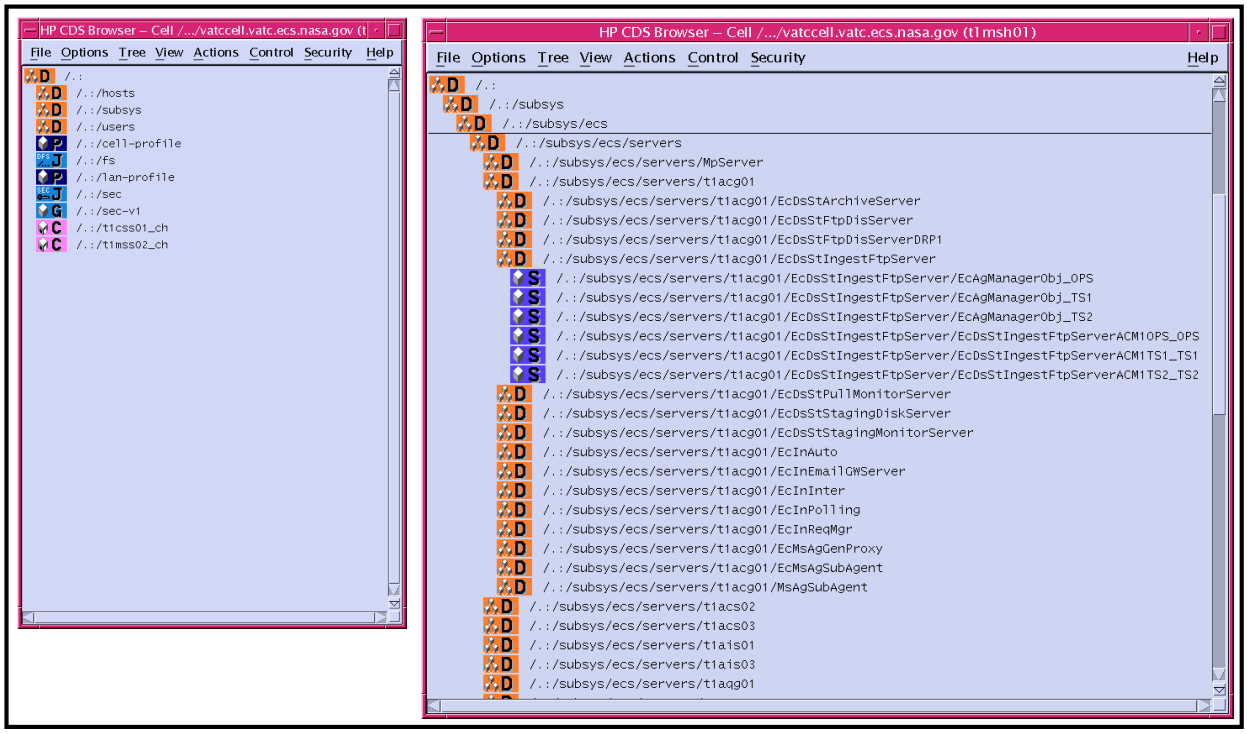


Figure 21. Screens from the cdsbrowser

Conduct the following procedure to use the *cdsbrowser to* check DCE entries for a server.

Using *cdsbrowser* to Check DCE Entries for a Server (Procedure 3.2)

1 Log-in to the *cdsbrowser* host (e.g., **e0msh03**, **g0msh08**, **l0msh03**, or **n0msh03**).

2 At the UNIX prompt, type **dce_login *UserID***, and then press the **Return/Enter** key.

- A **Password:** prompt is displayed.

3 At the **Password:** prompt, type **<*DCEPasswd*>B**, and then press the **Return/Enter** key.

- A UNIX prompt is displayed.
- NOTE: You can check that the DCE login is successful by typing **klist**, and the pressing the **Return/Enter** key; if the DCE login is successful, the logged in principal will be displayed, along with other DCE information.

4 Type **cd /opt/dce/bin** and then press the **Return/Enter** key.

- The prompt indicates a change to the **/opt/dce/bin** directory.

5 Type **cdsbrowser &**, and then press the **Return/Enter** key.

- The ***cdsbrowser*** initial GUI screen is displayed.

6 Double click on the **/subsys** line on the GUI.

- The screen shows the contents of the selected directory.

7 Double click on the **/subsys/ecs** line on the GUI.

- The screen shows ECS modes and servers.

8 Double click on the **/subsys/ecs/servers** line on the GUI.

- The screen shows the subsystem machines directories.

9 Double click on the **/subsys/ecs/servers/<*serverhost*>** line on the GUI.

- The screen shows the server directory for the selected <*serverhost*>.

10 Double click on the **/subsys/ecs/servers/<*serverhost*>/<*server*>** line on the GUI.

- The screen shows the server entries for the selected <*server*>. If DCE entries are missing, or if an entry shows an icon labeled "**o**" (for "object") instead of "**s**" (for "server"), have the DCE Administrator or Operations Supervisor restart DCE on the host for which entries are missing.
- If the DCE entries reflected in the *cdsbrowser* are OK, continue with the procedure for **Checking for Consistency between Calling and Called DCE Entries (Procedure 3.3)** (subsequent section of this lesson).

Checking for Consistency between Calling and Called DCE Entries

If a client cannot reach a server, it is possible that the client is calling with a name different from that in the DCE entry for that server. Use the following procedure to check for consistency.

Checking for Consistency between Calling and Called DCE Entries (Procedure 3.3)

1 Examine the debug log (**/usr/ecs/<*mode*>/CUSTOM/logs/<*server*>Debug.log**) of the server from which the call originated to determine the DCE entry being used for the called server, as reflected in the error message (e.g., "**Unable to reach /.:/subsys/ecs/servers/<*serverhost*>/<*server*>/<*servername*>**").

- Refer to the procedure for **Checking Server Log Files (Procedure 2.2)** (previous section of this lesson).

2 Compare the DCE entry noted in Step 1 with the DCE Entry for the called server reflected in the *cdsbrowser* or the called server **.CFG** file.

- Refer to the procedure for **Using *cdsbrowser* to Check DCE Entries for a Server** (**Procedure 3.2)** (previous section of this lesson), or, on the called server, use any UNIX editor or visualizing command (e.g., **vi**, **pg**, **more**, **tail**) to review the appropriate file (i.e., **/usr/ecs/<*mode*>/CUSTOM/cfg/<*server*>.CFG**).

3 If the DCE entry for the called server is different from the one being used by the server/client from which the call originates, ask the DCE Administrator to resolve the conflict.

Recovering from a Database Access Problem

Sybase is the database engine for most ECS data stores. If a server is unable to access the database, or if there is some other problem with Sybase, ECS operation will be impaired. Use the following procedure to recover from a database access problem.

Recovering from a Database Access Problem (Procedure 4.1)

1 Log-in to the Sybase host for the appropriate server.

- Hosts for the various Sybase servers at the different DAACs are listed in document 920-TD*x*-009, where *x* is **E** for **EDC, L** for **LaRC**, **G** for **GSFC**, or **N** for **NSIDC**.

2 Type **ps -ef | grep dataserver**, and then press the **Return/Enter** key.

- If active Sybase dataserver processes are displayed, go to Step 3.
- If no active Sybase dataserver processes are displayed, have the Database Administrator restart Sybase.

3 If examining processes on the Sybase host for SDSRV (e.g., **e0acg01**, **g0acg01**, **l0acg02**, **n0acg01**), it is important that the Sybase start time is prior to the start time of SQS. To check this, type **ps -ef | grep sqs**, and then press the **Return/Enter** key. (***Note***: If not on the host for SDSRV, this does not apply; go to Step 4.)

- If an active SQS process is displayed normally with a start time after the start time of the Sybase dataserver processes, go to Step 4.
- If SQS process start time is prior to the start time of the Sybase dataserver processes, have the Database Administrator restart SQS.

4 Log-in to the host for the appropriate application server.

- Hosts for the various custom applications at the different DAACs are listed in document 920-TDx-502, where x is **E** for **EDC, L** for **LaRC**, **G** for **GSFC**, or **N** for **NSIDC**; a short, easy-to-use hardware/software mapping is available as document 910-TDA-005.

5 Type **grep Sybase <*logfilename*>** to check for Sybase errors.

- Any Sybase entries in entries for the named logfile are displayed.

6 If one or more Sybase entries indicate an error condition, restart the server to re-establish the connection.

Recovering from a Missing Mount Point or Other File Access Problem

Correct functioning of ECS is dependent on client access to needed files, which may be in a remote network location. Often, server logs can be a source of error information that suggests a resolution for an access problem. Review of a server log may indicate, for example, that a server is using a particular path to look for a file that is not at that location. The resolution may be simply to ensure that the needed file is available in the location specified in the path. Access may also be prevented by permission restrictions. Examination of a server log may reveal a failed attempt to write to a database, resulting from incorrect permissions. The resolution in this case may be simply to use a different account with the correct permissions, or to have the Database Administrator or System Administrator reset the permissions.

Mount points provide remote access to shared file systems across networks, allowing a client to attach remote directory trees to a point within its local file system. If a mount point is lost, any of a client's ECS functions depending upon access through that mount point to files on a remote machine will be degraded or blocked. Use the following procedure to check for and recover from a missing mount point.

Recovering from a Missing Mount Point Problem (Procedure 5.1)

1 Log-in to the machine that the server is trying to access.

- Hosts for the various custom applications at the different DAACs are listed in document 920-TDx-502, where **E** for **EDC, L** for **LaRC**, **G** for **GSFC**, or **N** for **NSIDC**; a short, easy-to-use hardware/software mapping is available as document 910-TDA-005.

2 Type **cd /usr/ecs/<*mode*>/CUSTOM/<*HWCI*>/<*machine_name*>/data**, press the **Return/Enter** key, and then list the contents of the directory (i.e., type **ls** and then press the **Return/Enter** key).

- For **<*HWCI*>**, enter the name of the hardware configuration item directory to be accessed (the directory **/usr/ecs/<*mode*>/CUSTOM** may be listed to display available directories). For <***machine_name***>, enter the name of the directory for the host to be accessed.

3 If the **ls** command returns nothing, that indicates that the mount point is gone; the System Administrator will have to re-establish the mount point using standard procedure guidance in the appropriate Engineering Technical Directive.

Recovering from a Subscription Server Problem

Many elements of ECS functioning rely upon the health and correct operation of the Subscription Server (SBSRV). Archive insertions or deletions of data are accompanied by notification from the Science Data Server (SDSRV) to SBSRV, and in response, based on stored subscriptions, SBSRV initiates actions specified in the subscriptions. Therefore, if SBSRV is not functioning properly or if it is not communicating successfully with SDSRV or other ECS elements, ECS operations will be impaired. Use the following procedure to ensure that SBSRV is functioning properly or to recover from a problem with SBSRV.

Recovering from a Subscription Server Problem (Procedure 6.1)

1 Check to ensure that the subscription server is up and listening.

- Launch **ECS Assistant** on the Communications Subsystem (CSS) host and execute procedures to monitor the status of the subscription server and **cdsping all servers** using appropriate procedures.
- If the server is up and listening, go to Step 3.

2 If SBSRV is down or not listening, use the procedure **Stop an Application/Program** (Document 611-CD-510-001, Section 7.3.3) to stop the server, and then restart it using the procedure **Start an Application/Program** (Document 611-CD-510-001, Section 7.3.2).

3 Use the SBSRV GUI to add an FTPpush subscription for insertion of a small data file (e.g., AST_L1BT).

- Use appropriate procedures [e.g., **Fulfilling a Need for a One-Time Subscription** (Document 611-CD-510-001, Section 19.4.1)].

4 On the SBSRV host (i.e., ***x*0ins02**, where ***x*** is **g** for GSFC, **l** for LaRC, **e** for EDC, or **n** for NSIDC), type **cd /usr/ecs/<*mode*>/CUSTOM/cfg**, and then press the **Return/Enter** key.

- The prompt indicates change to the **/usr/ecs/<*mode*>/CUSTOM/cfg** directory.

5 Have the Database Administrator (DBA) log into Sybase using the UserName and Password that the server is using.

- Have DBA log on to the SBSRV database host (i.e., ***x*0ins01**, where ***x*** is **g** for GSFC, **l** for LaRC, **e** for EDC, or **n** for NSIDC). Then type **isql -UEcSbSubServer -S*x*0ins02_srvr**, then press the **Return/Enter** key, and, when prompted, enter the appropriate password.

- If the Sybase access attempt is successful, the ISQL prompt **1>** is displayed. Type **exit** and press the **Return/Enter** key.
- If the Sybase access attempt is not successful (i.e., the ISQL prompt is not displayed), it may be necessary to restart Sybase, using appropriate procedures (refer to **Database Administrator Responsibilities**, Document 611-CD-510-001, Section 4.3).

Recovering from Granule Insertion Problems

Successful data storage functions are the heart of ECS. Successful ingest of data or processing of data to produce new science data granules require that Storage Management (STMGT) is inserting the product into the archive and that Science Data Server (SDSRV) is inserting the associated metadata into the inventory. Staging disks and staging monitors for the Archive server and the Ingest FTP server are also involved in this process. To check the functioning of these elements, it is necessary that the ESDTs are installed and available, and that subscriptions have been registered as noted in previous sections of this lesson. Have the Ingest/Distribution Technician insert a small file. Then, use the following procedure to recover from granule insertion problems.

Recovering from Granule Insertion Problems (Procedure 7.1)

1 Log into the host for SDSRV (e.g., **e0acs05**, **g0acs03**, **l0acs03**, **n0acs04**) and review the server log (**EcDsScienceDataServerDebug.log**); refer to **Checking Server Log Files** (previous section of this lesson).

- Examine the section of the log with entries near the time of the problem, looking for error messages that indicate communication failure.
- If the log file entries indicate a communication problem, note the server(s) with which there is impairment or disruption of communication.
- Repeat this step for the Archive Server (e.g., on host ***x*0drg01** where ***x*** is **g** for GSFC, **l** for LaRC, **e** for EDC, or **n** for NSIDC) where the server log to examine is **EcDsStArchiveServerDebug.log**, and, as indicated in any entries referring to associated communications problems, **EcDsStStagingDiskServerDebug.log** and **EcDsStStagingMonitorServerDebug.log**.
- As indicated in any entries referring to associated communications problems, repeat this step for the Advertising Server (e.g., on host ***x*0ins02** where ***x*** is **g** for GSFC, **l** for LaRC, **e** for EDC, or **n** for NSIDC) where the server log to examine is **EcIoAdServerDebug.log**, and for the Subscription Server (e.g., on host ***x*0ins01** where ***x*** is **g** for GSFC, **l** for LaRC, **e** for EDC, or **n** for NSIDC) where the server log to examine is **EcSbSubServerDebug.log**.

- If there are no apparent communications problems, go to Step 2.
- Use appropriate procedures to resolve any communications problems (refer to **Recovering from a Connectivity/DCE Problem (Procedure 3.1)** (previous section of this lesson).

Note: To run the Check Archive script **EcDsCheckArchive**, it is necessary to enter eight database-specific parameters when prompted during the running of the script: STMGT SQL server name, STMGT database name, STMGT SQL server userID, STMGT SQL server database password, SDSRV SQL server name, SDSRV database name, SDSRV SQL server userID, and SDSRV database password. To facilitate the smooth execution of the script, the parameters may be set as environmental variables instead. The parameters are not readily available to most operators; therefore, you will need to obtain them from the Database Administrator or have the Database Administrator run the script for you, using steps 2 through 4.

2 On the host for the Archive Server (***x*0drg01**), type **cd /usr/ecs/<*mode*>/CUSTOM /utilities** and then press the **Return/Enter** key.

- The prompt reflects the directory change to **/usr/ecs/<*mode*>/CUSTOM/utilities**.

3 Type **EcDsCheckArchive <*mode*>**.

- The Check Archive script runs; the displayed information should be similar to the following:

```
============================================================
This script is designed to validate the Inventory
against the Archive.

The user must select the menu option associated with the
Volume Group to be validated

        Please press [RETURN] to continue
============================================================
```

4 Follow the on-screen prompts for the script, entering the necessary parameters.

- The script provides indication of any discrepancies between the presence of granules in the Archive and entries in the inventory (metadata). Note that the appearance of a discrepancy is not necessarily indication of a failure (e.g., if a granule has been deleted but the inventory database has not been cleaned up, there may be inventory entries for which there are no granules in the archive), but a problem may be indicated if a discrepancy is apparent for a granule that you just inserted. Note also that this script would not reveal a problem if you attempted to insert a granule which failed to get inserted and also had its metadata fail to be inserted into the inventory (i.e., no granule and no inventory entry = no discrepancy). Therefore, if the script reveals no discrepancies, it may still be useful to conduct a direct examination to determine if the granule has been inserted.

5 On the host for the Archive Server (***x*0drg01** [or ***x*0drg0*n***]), type the directory change command **cd /dss_stk1/<*mode*>/<*data_type_directory*>** and then press the **Return/Enter** key.

- The prompt indicates change to the **/dss_stk1/<*mode*>/<*data_type_directory*>** directory.

6 Type **ls -al | grep "<*date*>"** where **"<*date*>"** is a three-letter abbreviation for the month followed by a number indicating the day (e.g., **"Apr 21"**), and then press the **Return/Enter** key.

- If the inserted file is displayed, with date and time of entry, go to Step 7.
- If the inserted file is not displayed, have the Ingest/Distribution Technician insert the file again. If this succeeds (i.e., the file is now listed), go to Step 7; otherwise, have the Archive Manager conduct the procedure for **Recovery from Failure to Store or Retrieve Data** (Document 611-CD-510-001, Section 17.6.6).

7 Determine if the inserted file is reflected in the Inventory Database (Database Administrator function) by logging into Sybase on the host for SDSRV [use procedure similar to steps 4 and 5 of **Recovering from a Subscription Server Problem (Procedure 6.1)** (previous section of this lesson)] and then selecting the data type.

- If the inserted file is reflected in the Inventory Database, go to Step 8.
- If the inserted file is not reflected in the Inventory Database, perform the procedure for **Recovery from a Database Access Problem (Procedure 4.1)** (previous section of this lesson).

8 Determine if the directory from/to which the copy is being made is visible on the machine being used; check the mount points on the Archive host and the SDSRV host [use the procedure **Recovering from a Missing Mount Point Problem (Procedure 5.1)** (previous section of this lesson)].

- If the mount points are OK, go to Step 9.
- If necessary, re-establish the mount point(s).

9 If you inserted the file with the DSS Driver, go to Step 11. If you used Ingest to insert the file, on the Ingest host (e.g., **e0icg01**, **g0icg01**, **l0icg01**) examine the **drp**- or **icl**-mounted staging directory to determine if a staging disk was created. To do this, first type **cd /usr/ecs/<*mode*>/CUSTOM/drp/<*host*>/data/staging/user<*#*>** (or type **cd /usr/ecs/<*mode*>/CUSTOM/icl/<*host*>/data/StagingArea/user<*#*>**), then press the **Return/Enter** key.

- The prompt reflects a change to the specified directory. [***Note***: Be sure that you are checking the correct mount/host. Most ingests use Ingest subsystem staging areas (i.e., **icl**), but others may not. Media ingest (e.g., from D3 tape) typically involves staging in a **dip** area. For a polling ingest for data from EDOS, the polling directory may serve as the staging area. Some data are staged directly to working storage in the Data Server subsystem. If in doubt, consult Ingest/Archive personnel.]

10 Type **ls -al | more** and then press the **Return/Enter** key.

- Any staging areas are listed in output similar to the following sample:

```
-r--r--r--  1 cmshared cmshared  449984 Apr 17 1999 :SC:AM1ANC.001:2462:1.CCSDS
-r--r--r--  1 cmshared cmshared     384 Apr 17 1999 :SC:AM1ANC.001:2462:2.CCSDS
-r--r--r--  1 cmshared cmshared  225248 Apr 19 1999 :SC:AM1ATTF.001:2483:1.CCSDS
-r--r--r--  1 cmshared cmshared  154399 Apr 15 1999 :SC:L7CPF.001:1250:1.ASCII
-r--r--r--  1 cmshared cmshared  154399 Apr 20 1999 :SC:L7CPF.001:1599:1.ASCII
-r--r--r--  1 cmshared cmshared 5410105 Apr 15 1999 :SC:MIB2GEOP.001:2475:1.HDF-EOS
-r--r--r--  1 cmshared cmshared 5410105 Apr 16 1999 :SC:MIB2GEOP.001:2482:1.HDF-EOS
-r--r--r--  1 cmshared cmshared 5410105 Apr 14 1999 :SC:MIL1A.001:2423:1.HDF-EOS
-r--r--r--  1 cmshared cmshared  720100 Feb 29 2000 :SC:MOD00.001:2348:1.CCSDS
-r--r--r--  1 cmshared cmshared     384 Feb 29 2000 :SC:MOD00.001:2348:2.CCSDS.
```

- If a staging area for the inserted file appears at the end of the list, go to Step 11.
- If no staging area appears for the inserted file, it is possible that the ingest failed and that the staging area was immediately removed as part of clean-up. Check the Ingest logs (e.g., **EcInReqMgrDebug.log**, **EcInAutoDebug.log**, **EcInGranDebug.log**, or **EcInGranDebug**.log, depending on the type of Ingest) [refer to the procedure for **Recovering from an Ingest Problem (Procedure 9.1)** (subsequent section of this lesson)] to determine if a staging disk was created. If no staging disk was created, perform the procedure **Recovering from a Connectivity/DCE Problem (Procedure3.1)** (previous section of this lesson).

11 Have the Archive Manager ensure that the Archive volume groups are set up correctly [refer to **Use Storage Management GUIs to Display Archive Path Information** (Archive Lesson, 625-CD-010-002)].

12 Have the Archive Manager ensure that the volume groups are on line [refer to **Using the AMASS GUI to View Volume Group and Volume Information** (Archive Lesson, 625-CD-010-002)].

13 Examine the server logs to determine if the subscription was triggered by the insertion [refer to the procedure for **Checking Server Log Files (Procedure 2.2)** (previous section of this lesson)].

- On the SDSRV host (e.g., **e0acs05**, **g0acs03**, **l0acs03**, **n0acs04**), examine **EcDsScienceDataServerDebug.log** to determine if SDSRV sent a trigger (event notification); the entry should be similar to the following:

  05/06/99 12:51:53: DsBtSbsrvNotifier: Notification sent to sbsrv for INSERT of SC:AST_L1BT.001:2059.

- On the SBSRV host (e.g., **e0ins01**, **g0ins01**, **l0ins01**, **n0ins01**), examine **EcSbSubServer.ALOG** to determine if SBSRV received the trigger; the entry should be similar to the following:

  PID : 3020:MsgLink :0 meaningfulname :EcSbTriggerEventRequestTriggerTrigger
  Msg: Triggering event for EventID = 74 Priority: 0 Time : 05/06/99 12:51:54

PID : 3020:MsgLink :0 meaningfulname :EcSbTriggerEventRequestTriggerTrigger0
Msg: Firing subscriptions for event #74 Priority: 0 Time : 05/06/99 12:51:54

Note: EventID = 74 identifies the event as Insert of AST_L1BT. This information may be obtained from the list of events on the Subscription GUI, or by examining the **EcSbSubServerDebug.log** and noting the EventID specified there when the subscription was established.

Note: It is also possible to check for the SBSRV receipt of the trigger by examining **EcSbSubServerDebug.log**. However, the amount of information to be sifted in that log may complicate the task. If you choose to use **EcSbSubServerDebug.log**, you should look for entries similar to the following

05/06/99 12:51:54: EcSbTriggerEventRequest:Trigger: Triggering event for EventID = 74.
-
EVENTPARMS[UR(UR:10:DsShESDTUR:UR:15:DsShSciServerUR:13:[VTC:DSSDSRV]:20:SC:AST_L1BT.001:2201)
--UnnamedPL[
---CollectionDescriptionClass[ShortName(AST_L1BT) VersionID(1)]
---ECSDataGranule[SizeMBECSDataGranule(0.001000000047497451) ProductionDateTime(07/10/98 14:49:27)]
---SingleDateTime[TimeofDay(09:12:34.567890) CalendarDate(07/30/98)]
---SpatialDomainContainer[]
---AdditionalAttributes[
----AdditionalAttributesContainer[AdditionalAttributeName(ASTERGRANULEID)
-----InformationContent[
------ParameterValue[ParameterValue(ASTL1BT1997032015:00:01199703200001)]]]
----AdditionalAttributesContainer[AdditionalAttributeName(DAR_ID)
-----InformationContent[
------ParameterValue[ParameterValue(12345678)]]]] dbID(2201) type(SC) subType(AST_L1BT.001)
---nonScienceData[
----DATAFILEGROUP[userDataFile(tahoe-north-middle.MTA) internalFileName(:SC:AST_L1BT.001:2201:1.HDF-EOS) checkSum(0) fileSize(517) ArchiveID(DRP1_TS1:AST_L1BT.001) backupIdentifier() offsiteIdentifier() ESDTStatus(1) archiveDescription(None)]
----DATAFILEGROUP[userDataFile(tahoe-north-middle.hdf) internalFileName(:SC:AST_L1BT.001:2201:2.HDF-EOS) checkSum(0) fileSize(5410105) ArchiveID(DRP1_TS1:AST_L1BT.001) backupIdentifier() offsiteIdentifier() ESDTStatus(1) archiveDescription(None)]] SizeMBECSDataGranule(5.410622119903564)]]

- On the SBSRV host (e.g., **e0ins01**, **g0ins01**, **l0ins01**, **n0ins01**),, examine **EcSbSubServerDebug.log** to determine if SBSRV sent an acquire request to SDSRV; the entry should be similar to the following:

05/06/99 12:51:55: EcSbSubscription:Execute: Action = ACQUIRE :
-parameters[FTPUSER(jrattiga) FTPPASSWORD(abc123) FTPHOST(t1dps04) FTPPUSH DEST(/home/jrattiga/push) ECSUSERPROFILE(tester) DDISTNOTIFYTYPE(MAIL) DDIST MEDIATYPE(FtpPush) DDISTMEDIAFMT(FILEFORMAT)]
05/06/99 12:51:55: Execute acquire here
rpcID :---------- Dump of RPC ID ----------
Transaction ID: [fc6905d4-03d3-11d3-8f4a-c676e82eaa77]
Sub Transaction ID: [SDSV]
Readable tag: []
Server ID: [SBSV]
Subindex: [0]

05/06/99 12:51:56: new RpcID = ---------- Dump of RPC ID ----------
Transaction ID: [fc6905d4-03d3-11d3-8f4a-c676e82eaa77]
Sub Transaction ID: [SDSV]
Readable tag: []
Server ID: [SBSV]
Subindex: [1]

05/06/99 12:51:56: name = UR
05/06/99 12:51:56: === found UR =====
05/06/99 12:51:56: UR is ==> UR:10:DsShESDTUR:UR:15:DsShSciServerUR:13:[VTC: DSSDSRV]:20:SC:AST_L1BT.001:2201

- On the DDIST host (e.g., **e0dis02**, **g0dis02**, **l0dis02**, **n0dis02**), examine the log **EcDsDistributionServerDebug.log** to determine if an e-mail notification was sent to the user identified in the subscription; the output should be similar to the following:

05/06/99 12:52:41: Media::SendNotificationMessage.(myNotify,mySite,myConfig->GetMode(),mailAddress): (, , TS1, cmts1@t1ins02u.ecs.nasa.gov
Media::SendNotificationMessage: Getting e-mail address from configuration file.
05/06/99 12:52:41: DdDsDoneQueue::Thread Was marked SyncDone and Signaled. RequestID= 125125210220554

- If the subscription trigger activity is not reflected in the logs, or the log shows an error message indicating trigger failure, perform the procedure for **Recovering from a Subscription Server Problem (Procedure 6.1)** (previous section of this lesson).

- If the logs indicate that the subscription triggers worked properly, continue with the procedure for **Handling an Acquire Failure (Procedure 8.1)** (subsequent section of this lesson).

Handling an Acquire Failure

As a first check, it is appropriate to determine if the acquire request appears in the list of System Requests on the Science Data Server GUI. If the acquire request does not appear on the Science Data Server GUI, you will need to determine where the breakdown occurred. Diagnosing an acquire failure requires detailed examination of the following system log files and directories associated with the process:

- Science Data Server log file (EcDsScienceDataServerDebug.log).
- Archive Server log file (EcDsStArchiveServerDebug.log).
- Staging Area.
  - Presence of the relevant file.
  - Staging Disk log files (EcDsStStagingDiskServerDebug.log or EcDsStStaging MonitorServerDebug.log).
  - Space available in the staging area.

In addition, note that a number of servers, clients, or other software running on various hosts, as reflected in Table 3. Hosts, Servers, Clients and Other Software Relevant to Acquires, may be involved at various times in processing an acquire request. More information useful in troubleshooting may appear in related logs on these hosts.

Table 3. Hosts, Servers, Clients and Other Software Relevant to Acquires

HOST	SERVER/CLIENT/OTHER SOFTWARE
Distribution Server (e.g., x0dis02)	Distribution Server (EcDsDistribution Server) 8mm Server (EcDsSt8MMServer) D3 Server (EcDsStD3Server)
Working Storage (e.g., x0wkg01)	Archive Server (EcDsStArchiveServer) Staging Monitor Server (EcDsStStagingMonitorServer) Staging Disk Server (EcDsStStagingDiskServer)
SDSRV Server (e.g., x0acs03)	Science Data Server (EcDsScienceDataServer) HDF EOS Server (EcDsHdfEosServer)
Access/Process Coordinators (APC) Server (e.g., x0acg01)	Archive Server (EcDsStArchiveServer) FTP Distribution Server (EcDsStFtpDisServer) Staging Monitor Server (EcDsStStagingMonitorServer) Staging Disk Server (EcDsStStagingDiskServer) Pull Monitor Server (EcDsStPullMonitorServer)
FSMS Server (e.g., x0drg01)	Archive Server (EcDsStArchiveServer) Staging Monitor Server (EcDsStStagingMonitorServer) Staging Disk Server (EcDsStStagingDiskServer)
Interface Server 02 (e.g., x0ins01)	Subscription Server (EcSbSubServer) Event Server (EcSbEventServer)

Use the following procedure to:

- make the initial check on the Science Data Server GUI.
- follow up with checks of the Science Data Server log file and Archive Server log file.
- determine if a failure occurred during copying of the files to a staging area (and if so, whether there is sufficient staging space available).

Handling an Acquire Failure (Procedure 8.1)

1 Examine the System Requests displayed on the Science Data Server GUI to determine if SDSRV received the acquire request from SBSRV [use procedure **Monitor Science Data Server Request Processing** (Document 611-CD-510-001, Section 16.7.5)].

2 On the SDSRV Server host (e.g., e0acs05, g0acs03, l0acs03, n0acs04), review the server logs (**EcDsScienceDataServer.ALOG**, **EcDsScienceDataServerDebug.log**); refer to **Checking Server Log Files** (previous section of this lesson).

- Examine the section of the log with entries near the time of the problem, looking for messages that indicate whether the relevant file was successfully acquired.

- The **EcDsScienceDataServer.ALOG** file should contain entries identifying the file to be acquired by the ShortName of the corresponding ESDT; entries should be similar to the following:

PID : 29168:MsgLink :0 meaningfulname :DsSrSessionExecuteRequestStart0
Msg: Request ID b5156038-03d3-11d3-8d16-c676e82eaa77:????: executing:
DsSrRequest (1): DsShSciRequestImp: [svr: ScienceDS, pri: NORMAL domain:]:
(DsShSciCommandImp: service: INSERT num parameters: 3 category: Parameters are:
-UnnamedPL[SHORTNAME(AST_L1BT) VERSIONID(001)
--MAINGROUP[SHORTNAME(AST_L1BT) VERSIONID(001)
---METAFILEGROUP[METADATAFILE(/home/cmops/data/SCAST_L1BT.0011279.met)]
---DATAFILEGROUP[DATAFILE(/home/cmops/data/tahoe-north-middle.MTA)]
---DATAFILEGROUP[DATAFILE(/home/cmops/data/tahoe-north-middle.hdf)]]]
WC)

- The **EcDsScienceDataServerDebug.log** file should contain entries regarding the acquire activity. The following types of messages should be included in the log file:

05/06/99 12:52:01:
About to execute Statement: exec ProcInsertReqDomain 2205, "UR:10:DsShESDT UR:UR:15:DsShSciServerUR:13:[VTC:DSSDSRV]:20:SC:AST_L1BT.001:2201"
05/06/99 12:52:01:
About to execute Statement: ProcInsertAcquireCmd 2206, 2205, 3, null, null, "tester", "FtpPush", "MAIL", "FILEFORMAT", null, "jrattiga", "abc123", "t1dps04", "/home/jrattiga /push", null, null

- If the ShortName does not appear in the file, with a timestamp corresponding to the time of the attempted acquire, SDSRV may not be running, or may not be communicating with other servers. Check to be sure the server is up [refer to **Using HP OpenView to Check the Status of Hosts and Servers** (previous section of this lesson)] and, if appropriate, check for connectivity problems [refer to **Recovering from a Connectivity/DCE Problem** (previous section of this lesson)].

- If the log file does contain entries for the relevant ShortName, and indicates that two files (the file and its associated metadata file) are being distributed, SDSRV has completed its role in the acquire. Go to the next step.

- If the ALOG contains the ShortName, and also contains an error showing that the data file time stamp does not match the time stamp required by the acquire, the data file needs to be removed from the Science Data Server and reinserted.

  – This is usually done using a script called DsDbCleanGranules.

3 To inspect the Archive Server log for error messages associated with the acquire, on the Archive host (e.g., **e0drg01**, **g0drg01**, **l0drg01**, **n0drg01**), review the server log (**EcDsStArchiveServerDebug.log**); refer to **Checking Server Log Files** (previous section of this lesson).

- Examine the section of the log with entries near the time of the problem, looking for messages that indicate whether the relevant file was successfully acquired.
- If the log indicates that the relevant file was successfully acquired, go to the next step.
- If the file was not successfully acquired, have the Archive Manager perform the procedure **Recovery from Failure to Store or Retrieve Data** (Document 611, Section 17.6.6) to troubleshoot and correct any AMASS problems.

4 To determine whether the file being acquired (or a link to it) and its associated metadata file arrived in the Data Distribution staging area, on the Distribution Server (e.g., **e0dis02**, **g0dis02**, **l0dis02**, **n0dis02**) type **cd /usr/ecs/<*mode*>/CUSTOM/drp/<*archivehost*>/data/staging/user<#>** and then press the **Return/Enter** key.

- The prompt indicates the change to the specified directory.

5 Type **ls -lrt** and then press the **Return/Enter** key.

- The contents of the directory are displayed.

6 Review the listing to determine whether the relevant file and its metadata file arrived in the staging area.

- The display should contain entries similar to the following:

```
lrwxrwxr-x  1 cmshared cmshared  75 Apr 26 12:52 L7CPF19980518_19980518.01 ->
/usr/ecs/TS1/CUSTOM/drp/raven/data/staging/user1/:SC:L7CPF.001:1427:1.ASCII
-rw-rw-rw-   1 cmshared cmshared   14802 Apr 26 12:52 SCL7CPF.0011427.met
-rw-rw-r--   1 cmshared cmshared    111 Apr 26 13:01 staging.disk.filename.list
-rw-rw-r--   1 cmshared cmshared   2044 Apr 26 13:01 PACKING.LST.115124935248431
```

- If the relevant files were not successfully staged, the staging log files may reveal the cause; go to Step 7.
- If the relevant files were successfully staged, an acquire failure could be a result of problems with related servers or software (see Table 1). Ensure that the necessary hosts and servers are up [refer to **Using HP OpenView to Check the Status of Hosts and Servers** (previous section of this lesson)].

7 To inspect the Staging Disk log for error messages associated with the acquire, on the APC Server host (e.g., **e0acg01**, **g0acg01**, **l0acg02**, **n0acg01**), review the server logs (e.g., **EcDsStStagingDiskServerDebug.log**; **EcDsStStagingMonitorServerDebug.log**); refer to **Checking Server Log Files** (previous section of this lesson).

- Examine the section of each log with entries near the time of the problem, looking for messages that indicate whether the relevant files were successfully staged.
- If the relevant files were not successfully staged, the cause may be a lack of space in the staging area; go to Step 8.
- If the relevant files were successfully staged, an acquire failure could be a result of problems with related servers or software (see Table 1). Ensure that the necessary hosts and servers are up [refer to **Using HP OpenView to Check the Status of Hosts and Servers** (previous section of this lesson)].

8 To check the space available in the staging area, on the Distribution Server (e.g., **e0dis02**, **g0dis02**, **l0dis02**, **n0dis02**) type **cd /usr/ecs/<*mode*>/CUSTOM/drp/<*archivehost*>/data** and then press the **Return/Enter** key.

- The prompt indicates the change to the specified directory.

9 Type **df -k .** (be sure to include the "**.**") and then press the **Enter** key.

- The filesystem, staging disk space capacity in kbytes, amount used, amount available, and percent of capacity are displayed, as in the following example:

```
Filesystem            kbytes    used   avail capacity  Mounted on
t1drg01:/usr/ecs/TS1/CUSTOM/drp/t1drg01/data
                      225209856 173253056 51956800    77%
/data1/ecs/TS1/CUSTOM/drp/t1drg01/data
```

- If there is not adequate space for staging the relevant files, it will be necessary to free up additional space (e.g., by purging expired files from cache).

Recovering from Ingest Problems

Ingest problems may vary significantly, with symptoms manifested that are specific to the type of Ingest being attempted. If a problem occurs, there is usually helpful information available on the Ingest GUI and it should be examined first. Ingest's many interfaces with other ECS subsystems mean that ingest problems may be traced not only to the Ingest subsystem itself, but also to numerous other ECS subsystems. Moreover, Ingest has interfaces with external data providers, and therefore problems may often be traced to communications with them. The Ingest lesson (Document 625-CD-008-002) provides detailed information on tracing Ingest problems, and if a problem occurs, the Ingest Technician/Archive Manager may often be able to resolve it through application of some of the procedures described in that lesson. Specifically, the Ingest Technician/Archive Manager should initially examine error indications and data available on the Ingest GUI and review relevant log files for error indications, including logs for the Ingest GUI, the Ingest Request Manager, the Ingest Granule Server, and the relevant Ingest Client. Ingest personnel can also perform procedures for:

- **Recovering from a Faulty DAN**.
- **Recovering from Exceeding the Volume Threshold**.
- **Recovering from Exceeding the Maximum Number of Concurrent Requests**.
- **Recovering from Insufficient Disk Space**.
- **Recovering from Exceeding the Expiration Date/Time Period**.
- **Recovering from File Transfer (ftp) Error**.
- **Recovering from Processing Errors**.

If they are unable to solve the problem, there may be some additional troubleshooting related to granule insertion that will be helpful. After Ingest personnel exhaust relevant troubleshooting procedures from the Ingest lesson (Document 625-CD-008-002), use the following procedure to ensure that the manifested Ingest Problem does not reflect granule insertion problems. If the problem cannot be identified and fixed without help within a reasonable period of time, the appropriate response is to call the help desk or submit a trouble ticket in accordance with site Problem Management policy.

Recovering from Ingest Problems (Procedure 9.1)

1 Have the Ingest Technician perform a test ingest of an appropriate type (i.e., polling ingest of MODIS L0 data, ingest of AST_L1BT data from D3 tape, polling ingest of Attitude data without delivery record, polling ingest of L7 IAS data with delivery record, auto ingest of L7 Format 1 and Format 2 data), depending on the type of ingest associated with the problem.

2 Ensure that the insertion worked normally and that the insertion is reflected in the Archive and Inventory Databases, and perform any necessary corrective actions if the insertion did not work.

- Use the procedure for **Recovering from Granule Insertion Problems (Procedure 7.1)** (previous section of this lesson).

Recovering from PDPS Plan Creation/Activation and PGE Problems

Many ECS functions, particularly those related to the Planning and Data Processing Subsystems (PDPS), are dependent on correct registration and functioning of the science algorithms, or Product Generation Executives (PGEs). The initiation of successful PDPS functions is dependent on the ability to create and activate production plans. The correct functioning of PGEs is in turn dependent on the functioning of SDSRV and STMGT in data insertion and archiving, as well as related communications. If there is a production planning problem, planning personnel have some initial troubleshooting that they can do using the guidance in **Troubleshooting Production Planning Problems** (Production Planning and Processing Lesson, Document 625-CD-006-002). Production personnel may apply guidance for **Troubleshooting Processing Problems** (Production Planning and Processing Lesson, Document 625-CD-006-002). If they are unable to resolve the problem, additional troubleshooting may be necessary. Troubleshooting PGE problems typically includes inserting a small file to check that data insertion and archiving functions are working, as well as checking PDPS mount points and then examining PDPS and SDSRV logs to search for evidence of communications failure during PGE execution. It may also be helpful to have PDPS personnel create and activate a plan using sample PGEs such as ETS and ACT. Use the following procedure to recover from problems with plan creation or activation and the running of PGEs.

Recovering from PDPS Plan Creation/Activation and PGE Problems (Procedure 10.1)

1 Examine the server logs to determine if PDPS communicated with SDSRV during the PGE execution associated with the problem, using the procedure for **Checking Server Log Files (Procedure 2.2)** (previous section of this lesson).

- On the host for the Queuing Server (**e0sps04**, **g0sps06**, **l0sps03**, or **n0sps08**), examine **EcDpPrJobMgmtDebug.log** and **EcDpPrDeletionDebug.log**.
- On the host for SDSRV (**e0acs05**, **g0acs03**, **l0acs03**, or **n0acs04**), examine **EcDsScienceDataServerDebug.log**.
- If the logs indicate evidence of communication failure, perform the procedure for **Recovering from a Connectivity/DCE Problem (Procedure 3.1)** (previous section of this lesson); if the log suggests a database access failure, perform the procedure for **Recovering from a Database Access Problem (Procedure4.1)** (previous section of this lesson).

2 Ensure that PDPS personnel have thoroughly reviewed the problem using procedures for **Troubleshooting Processing Problems** [refer to Production Planning and Processing Lesson (Document 625-CD-006-002)].

- When a PGE binary fails, a failed PGE granule is stored in the archive; this is essentially a tar file of the PDPS run-time directory. It may be helpful to retrieve the relevant failed PGE granule from the archive and examine the information for indications of the problem. If there is indication of a problem with the PGE binary, it may be necessary to refer the problem to SSI&T personnel for solution.

3 Insert a small file using the DSS Driver.

- The DSS driver is used for inserting data into the data server (archive), performing acquires from the archive, and/or searching the archive for granules. It is launched by running a script, **EcTsDsClientDriverStart**, on the SDSRV host (**e0acs05**, **g0acs03**, **l0acs03**, or **n0acs04**). Then you follow prompts on the screen to specify data insert, main data type, any accompanying metadata, and filename(s).

4 Ensure that the insert into the SDSRV database and Archive worked and that the insertion is reflected in the Archive and Inventory Databases, and perform any necessary corrective actions if the insertion and associated triggers did not work.

- Use the procedure for **Recovering from Granule Insertion Problems (Procedure 7.1)** (previous section of this lesson).

5 Determine if the Planning and Data Processing Subsystems (PDPS) mount point is visible on the SDSRV host (**e0acs05**, **g0acs03**, **l0acs03**, or **n0acs04**) and on the Archive Server host (**e0drg01**, **g0drg01**, **l0drg1**, or **n0drg01**) by following the procedure for **Recovering from a Missing Mount Point Problem (Procedure 5.1)** (previous section of this lesson).

6 To check out PDPS functions, have planning personnel create and activate a plan to run ACT and ETS PGEs, using applicable procedures to create production requests [refer to the procedure **Create New Production Request** (Document 611-CD-510-001, Section 13.1.2)] and to create and activate the plan [refer to the procedure **Create New Production Plan** (Document 611-CD-510-001, Section 13.2.3)].

- Ensure that the necessary input and static files are present in SDSRV, using as guidance Steps 2, 3, and 4 of the procedure for **Recovering from Granule Insertion Problems (Procedure 7.1)** (previous section of this lesson).
- Ensure that the necessary ESDTs (e.g., for AST_09T, AST_08, and AST_05) are installed, using applicable procedures [e.g., **Recovering from Problems with ESDTs, DAP Insertion, SSI&T (Procedure12.1)** (subsequent section of this lesson) and **Add Science Data Server Data Types** (Document 611-CD-510-001, Section 16.7.3)].
- Ensure that there is a subscription for AST_08 FTPpush entered into SBSRV, using appropriate procedures [e.g., **Fulfilling a Need for a One-Time Subscription** (Document 611-CD-510-001, Section 19.4.1)].

7 On the Queuing Server host (**e0sps04**, **g0sps06**, **l0sps03**, or **n0sps08**) or the Science Processor host (**e0spg01**, **g0spg01**, **l0spg01**, or **n0sps03**), check the PDPS run-time directories, as follows:

- Type **cd /usr/ecs/<*mode*>/CUSTOM/pdps/<*processor_host*>/data/DpPrRm/<*processor_host*>_disk/<*PGE_directory*>/<*PGE#version_no.*>** and the press the **Return/Enter** key.
- List the files (i.e., type **ls -al | more** and then press the **Return/Enter** key). ***Note***: At the completion of a successful or unsuccessful PGE run, its run-time directory is cleaned up. Therefore, you will only see run-time directories for PGEs that are currently running or for which execution has been stopped. If execution is stopped, conduct troubleshooting in accordance with procedures for **Handling a Job that is Hanging in AutoSys** [refer to Production Planning and Processing Lesson (Document 625-CD-006-002)].

8 Determine if the user in the subscription received an e-mail message concerning the FTPpush [refer to Step 13 of the procedure for **Recovering from Granule Insertion Problems (Procedure7.1)** (previous section of this lesson)].

9 Determine if the files were pushed to the correct directory [refer to the procedure for **Recovering from Data Distribution Problems (Procedure14.1)** (subsequent section of this lesson)].

10 Execute *cdsping* of machines with which DDIST communicates from ***x*0dis02** [refer to the procedure for **Using ECS Assistant to Monitor Server Status** (Document 611-CD-510-001, Section 3.7.3.2)].

- It may be necessary to reboot any machine(s) from which there is no response [refer to the procedure for **Warm - By Subsystem Startup** (Document 611-CD-510-001, Section 3.1.1.2)].

Recovering from QA Monitor Problems

The Quality Assurance (QA) Monitor GUI is used to record the results of a QA check on a science data product, updating the QA flag in the metadata. This function is dependent on the presence in SDSRV of the data to be evaluated for quality. The operator uses the tool to execute a query of SDSRV to locate and retrieve the data (and/or its production history), and to return the results of the QA assessment in a metadata update. Some problems may result in the display of user messages; these are identified in Appendix A of the Operations Tools Manual (Document 609-CD-510-002, Table A.2.9-7) along with potential impacts, causes, and corrective actions. Most of the QA Monitor user messages result from problems with system communications or run-time errors, and the proposed corrective actions for the operator are often to exit the GUI and try again later. For other problems related to the system query, use the following procedure.

Recovering from QA Monitor Problems (Procedure 11.1)

1 Ensure that the data on which to perform QA are in the SDSRV.

- On the host for the Archive Server (***x*0drg01**), type the directory change command **cd /dss_stk1/<*mode*>/<*data_type_directory*>** and then press the **Return/Enter** key.
  - The prompt indicates change to the **/dss_stk1/<*mode*>/<*data_type_directory*>** directory.
- Type **ls -al | more** and then press the **Return/Enter** key.
  - A list of files is displayed, showing date and time of entry for each.
  - If the desired file is displayed in the list, go to Step 2.
  - If the desired file is not displayed, have the inserted again (e.g., from processing). If this succeeds (i.e., the file is now listed), go to Step 2; otherwise, have the Archive Manager conduct the procedure for **Recovery from Failure to Store or Retrieve Data** (Document 611-CD-510-001, Section 17.6.6).

2 On the host for SDSRV (e.g., **e0acs05**, **g0acs03**, **l0acs03**, **n0acs04**), examine the SDSRV logs (i.e., **EcDsScienceDataServer.ALOG**, **EcDsScienceDataServerDebug.log**). Use the procedure for **Checking Server Log Files (Procedure2.2)** (previous section of this

lesson) and look for evidence that the data query from the QA Monitor GUI was successfully received.

- If the log shows that SDSRV received the query, go to Step 3.
- If there is no entry indicating the query, log in to the host for the QA Monitor GUI (e.g., **e0pls03**, **g0pls01**, **l0pls02**, **n0pls02**) and examine the QA Monitor GUI logs (i.e., **EcDpPrQaMonitorGUI.ALOG**, **EcDpPrQaMonitorDebug.log**). Use the procedure for **Checking Server Log Files** (previous section of this lesson) and look for evidence of a communications failure. If necessary, perform the procedure **Recovering from a Connectivity/DCE Problem (Procedure3.1)** (previous section of this lesson).

3 On the host for the QA Monitor GUI (e.g., **e0pls03**, **g0pls01**, **l0pls02**, **n0pls02**), examine the QA Monitor GUI logs (i.e., **EcDpPrQaMonitorGUI.ALOG**, **EcDpPrQaMonitor Debug.log**). Use the procedure for **Checking Server Log Files (Procedure2.2)** (previous section of this lesson) and look for evidence that the query results were returned from SDSRV.

- If the log shows that the query was not returned, log in to the host for SDSRV (e.g., **e0acs05**, **g0acs03**, **l0acs03**, **n0acs04**) and examine the SDSRV logs (i.e., **EcDsScienceDataServer.ALOG**, **EcDsScienceDataServerDebug.log**). Use the procedure for **Checking Server Log Files** (previous section of this lesson) and look for evidence of a communications failure. If necessary, perform the procedure **Recovering from a Connectivity/DCE Problem (Procedure 3.1)** (previous section of this lesson).

Recovering from Problems with ESDTs, DAP Insertion, or SSI&T

Each ECS data collection is described by an Earth Science Data Type (ESDT), made known to the system by an ESDT descriptor file and associated software code which is built into the Data Server's dynamic link library (DLL) to perform the services. The ESDT descriptor is composed of sections containing the following information:

- Collection level metadata attributes with values contained in the descriptor.
- Granule level metadata attributes whose values are supplied primarily by the Product Generation Executives (PGEs) during runtime.
- Valid values and ranges for the attributes.
- List of services for the data and events that trigger responses throughout the system.

The ESDTs for all data collections to be input to or output from the PGEs must be built and registered in ECS data server software before any of the PGEs can be run under the automated processing system. Any corruption or other problem with an ESDT descriptor or related files may cause degradation or disruption of ECS functioning.

Delivered Algorithm Packages (DAPs) are the means by which ECS receives new Science Software. The insertion of a DAP is dependent on an appropriate ESDT being installed, but otherwise, the Ingest and insertion of DAPs, and the handling of DAP acquires for Science Software Integration and Test (SSI&T), share features with other insertions and acquires. Accordingly, troubleshooting of problems with DAP insertion and acquires follows procedures similar to those for troubleshooting of other insertions and acquires.

Tools and GUIs for Science Software Integration and Test (SSI&T) are essential for the testing of new science algorithms and for preparing them for integration into the ECS operating environment. If these tools and GUIs are not properly installed, or if the system cannot perform inserts and FTPpush functions, SSI&T will be prevented or degraded. The SSI&T process entails testing new PGEs for data processing, and therefore many SSI&T problems are problems with PGEs. Accordingly, useful guidance may be found in troubleshooting procedures applicable to processing problems (refer to **Troubleshooting Processing Problems** in the Production Planning and Processing Lesson, Document 625-CD-006-002) or problems with PGEs (refer to **Recovering from Planning and Data Processing Problems (Procedure 10.1)**, previous section of this lesson). Additional useful guidance may be found in the Science Software Integration and Test Lesson (refer to **Appendix A. Troubleshooting and General Investigation**, Document 625-CD-016-002). If these approaches do not readily resolve the problem, the following procedure may help ensure that the relevant software components are properly installed, DAPs can be inserted or acquired, and pushes from SDSRV are working to support SSI&T.

1 Check to ensure that involved subsystems and their computer software configuration items (CSCIs) are correctly installed and that the associated servers are functioning.

- Launch the Science Data Server (SDSRV) GUI and review the ESDTs listed on the **Data Types** tab in the **Names** column to ensure that there is an ESDT for the data to be inserted (e.g., via Ingest, Processing, or other insertion). Use appropriate procedures (e.g., from Document 611-CD-510-001, Section 16.7.1 **Starting the Science Data Server Operator GUI** and Section 16.7.2 **View the Science Data Server Data Type Information**). If the needed ESDT is not available, it may be necessary to install or re-install it using appropriate procedures (e.g., from Document 611-CD-510-001, Section 16.7.3 **Add Science Data Server Data Types**).

- Launch the Subscription Server (SBSRV) GUI and review the registered **Events** to ensure that the event associated with the problem is registered. Use appropriate procedures (e.g., from Document 611-CD-510-001, Section 19.4.2 **Fulfilling a Need for an Open-Ended Subscription**). If the event is not registered, it may be necessary to install or re-install the associated ESDT using appropriate procedures (e.g., from Document 611-CD-510-001, Section 16.7.3 **Add Science Data Server Data Types**).

- At the host for IOS and DDICT (e.g., **e0ins01**, **g0ins02**, **l0ins02**, **n0ins02**), launch the ECS Assistant and check for the presence of installed components and functioning of related servers for IOS and DDICT. Use appropriate procedures (e.g., from a previous section of this lesson, **Starting ECS Assistant** and **Using the ECS Assistant Server Monitor**. If **EcIoAdServer** or **EcDmDictServer** is not "up," restart the server(s) using appropriate procedures [e.g., **Start an Application/Program** (Document 611-CD-510-001, Section 7.3.2)].

- Ensure that Data Processing Subsystem and its computer software configuration items (CSCIs) are correctly installed [i.e., use ECS Assistant on the AIT Workstation (e.g., **e0ais02**, **g0ais05**, **l0ais09**) to check installed components for the Algorithm Integration and Test Tools; refer to procedure **Using ECS Assistant to Monitor Server Status** (Document 611-CD-510-001, Section 3.7.3.2)].

- If the items are not correctly installed, it may be necessary to reinstall the software; e.g., refer to **Handling an ESDT Installation Failure** (Appendix A of the Science Software Integration and Test Lesson, Document 625-CD-016-002).

2 Ensure the registration of events for any ESDT associated with the problem.

- On the SDSRV GUI, locate the ESDT either by scrolling through the list, or by typing all or part of the event name in the **Find** field and then clicking on the **Find** button. Click on the ESDT, and then click on the **View** button to display the **Descriptor Information** for the ESDT. In the **Descriptor Information** window, scroll to the end of the displayed information and review the last few lines to see the event data (**GROUP=EVENT**). Typically, there will be information for three types of events:
  - Insert.
  - Delete.
  - Update Metadata.

  You may also check for the presence of events by checking or asking the Database Administrator to check for their presence in the Science Data Server Database on the SDSRV database host (**g0acg01**, **l0acg02**, **n0acg01**, **e0acg01**).
- If no events are listed for the ESDT associated with the problem, or there seems to be a problem with event information available through the SDSRV GUI, it may be necessary to re-install the ESDT, using appropriate procedures (e.g., from Document 611-CD-510-001, Section 16.7.3 **Add Science Data Server Data Types**).

3 Review the SDSRV log files to determine if there were any errors associated with communications between SDSRV and IOS, SBSRV, or DDICT.

- Use appropriate procedures [e.g., **Checking Server Log Files (Procedure 2.2)** (previous section of this lesson)]. If there are indications of communication failure, check for connection or DCE problems [refer to **Recovering from a Connectivity/DCE Problem (Procedure 3.1)** (previous section of this lesson)].

4 If necessary, perform collection mapping for the Data Dictionary (DDICT).

- When an ESDT is re-installed, or when a new ESDT is installed, use the Data Dictionary Maintenance Tool (DDMT) to update the mapping for all collections. If this step is omitted, the system will not function correctly. [Refer to the procedure for **Update Data Dictionary Attribute/Keyword Mapping** (in User Services Lesson, 625-CD-013-002).]

5 Ensure that it is possible to insert into the SDSRV database and Archive and that the insertion is reflected in the Archive and Inventory Databases, and perform any necessary corrective actions if the insertion did not work.

- Use the procedure for **Recovering from Granule Insertion Problems (Procedure 7.1)** (previous section of this lesson).

6 Ensure the presence of the DAP or relevant data in the archive and that SDSRV can perform FTPpushes.

- Use the procedure for **Recovering from Data Distribution Problems (Procedure 14.1)** (subsequent section of this lesson).

Recovering from Problems with Data Search and Order

Data search functions are critical for user access to ECS collections. Data search is dependent on data being present in the Archive and reflected in the inventory, either as a result of ingest operations or as products of data processing.

Data search functions, as well as other ECS Operations, rely on correct functioning of the V0 Gateway (V0GTWY) and the Data Dictionary (DDICT), and on up-to-date mapping of valid attributes and keywords for the collections to be searched. It is therefore important to make certain that there is connectivity between V0GTWY and DDICT, and that they are able to communicate.

Data order by a registered user must function correctly if ECS products are to be distributed. Data order is dependent on successful data search. In addition, SDSRV must be able to support distribution by various means (e.g., FTPpull, FTPpush, media), and the account and any directory to be used by FtpDis must be valid. Use the following procedure to recover from problems with functions for data search, including connectivity between the V0GTWY and DDICT, and data order by a registered user.

Recovering from Problems with Data Search and Order (Procedure 13.1)

1 Ensure that appropriate data have been ingested and/or produced and are in SDSRV.

- On the host for the Archive Server (***x*0drg01** [or ***x*0drg0*n***]), type the directory change command **cd /dss_stk1/<*mode*>/<*data_type_directory*>** and then press the **Return/Enter** key.
  - The prompt indicates change to the **/dss_stk1/<*mode*>/<*data_type_directory*>** directory.
- Type **ls -al | grep <*granuleUR*>** and then press the **Return/Enter** key.
  - If the appropriate file(s) are displayed in the list, with date and time of entry for each, go to Step 2.
  - If appropriate file(s) are not displayed, have the file(s) inserted again (e.g., from Ingest or Processing). If this succeeds (i.e., file(s) are now listed), go to Step 2; otherwise, have the Archive Manager conduct the procedure for **Recovery from Failure to Store or Retrieve Data** (Document 611-CD-510-001, Section 17.6.6).

2 On the host for SDSRV (e.g., **e0acs05**, **g0acs03**, **l0acs03**, **n0acs04**), examine **EcDsScienceDataServerDebug.log** for evidence of problems with search activity.

- If there is an error message indicating "Archive center not available . . .," it may be necessary to "Update All Collections" using the button for that update on the Map Attributes tab of the Data Dictionary Maintenance Tool.

3 On the V0GTWY host (i.e., ***x*0ins02**, where ***x*** is **g** for GSFC, **l** for LaRC, **e** for EDC, or **n** for NSIDC), type **cd /usr/ecs/<*mode*>/CUSTOM/logs**, and then press the **Return/Enter** key.

- The prompt indicates a change to directory **/usr/ecs/<*mode*>/CUSTOM/logs**.

4 To view the V0GTWY debug log, type **more EcDmV0ToEcsGatewayDebug.log** and then press the **Return/Enter** key. [This procedure uses the **more** command, but any UNIX editor or visualizing command (e.g., **vi**, **pg**, **view**, **tail**) may be used to view the file.]

- This displays the file contents. Near the beginning, with date and time reflecting server start-up, the file should contain a **SQL SELECT** entry similar to:

  04/07/99 16:02:39: ~~~SQL STATEMENT IS: SELECT distinct t1.collectionId,t1.siteId,t1.ShortName, upper(t4.keywordName), t1.VersionID,t1.ArchiveCenter FROM DmDdECSCollection t1, DmDdInfoMgrCollXref t2, DmDdEquivalentAttributes t3, DmDdStringDomain t4, DmDdAttributeXref t5 WHERE t1.collectionId = t2.collectionId AND t1.siteId = t2.siteId AND upper(t1.LongName) = "LANDSAT-7 LEVEL-0R WRS-SCENE" AND t2.infoMgrName = "[MDC:DSSDSRV]" AND t5.siteId = t1.siteId AND t5.collectionId = t1.collectionId AND t5.collectionIdRef=t3.collectionId AND t5.siteIdRef=t3.siteId AND t5.attributeIdRef=t3.attributeId AND t4.collectionId=t3.collectionId AND t4.siteId=t3.siteId AND t4.attributeId=t3.attributeId AND 3.equivalentAttributeName= "DATASET_ID"

  and, further down in the output, still with date and time reflecting server start-up, the file should contain an entry similar to the following:

  04/07/99 16:02:43: End of StartMonitoring.

  If the start-up information is correct, it indicates that the V0GTWY is using a valid isql query; go to Step 3.

- If the log does not display start-up information, there may be a problem with DCE; refer to the procedure for **Recovering from a Connectivity/DCE Problem (Procedure 3.1)** (previous section of this lesson).

- If the log displays only part of the information (e.g., does not contain an entry for **End of StartMonitoring**), there may be a problem with the configuration file (**EcDmV0ToEcsGateway.CFG**), or with port assignment. It may be necessary to

reload the configuration file, or to re-assign ports to eliminate a conflict and then stop and restart the V0GTWY server; use the procedure **Stop an Application/Program** (Document 611-CD-510-001, Section 7.3.3) to stop the server, and then restart it using the procedure **Start an Application/Program** (Document 611-CD-510-001, Section 7.3.2).

5 Ensure that there is compatibility between the collection mapping database being used by the ECS Data Dictionary and the EOS Data Gateway Web Client.

- Ensure that collection mapping has been performed with the Data Dictionary Maintenance Tool after any removal, installation, or re-installation of ESDTs [use the procedure **Update Data Dictionary Attribute/Keyword Mapping** (in User Services Lesson, 625-CD-013-002)].
- Contact the EOSDIS V0 Information Management System (IMS) to ensure that any recently exported ECS valids have successfully passed their two-week valids update cycle and that the changes are currently operational. If the changes are not operational, it will be necessary to re-initiate the data search after the V0 IMS has implemented the changes.

6 To begin a check on functions for data order by a registered user, use the Data Distribution (DDIST) GUI to determine if DDIST is handling a request for the data and to monitor the progress of the request [refer to the procedure for **Monitoring/Controlling Data Distribution Requests (**Document 611-CD-510-001, Section 18.2.2)].

- The DDIST GUI may provide error messages to which the Distribution Technician can respond [refer to Appendix A of *Operations Tools Manual* (Document 609-CD-510-002, Table A.2.4-2)], and there are actions for troubleshooting data distribution problems that the Archive and/or Distribution personnel can perform [refer to procedure for **Recovering from a Data Distribution Failure** (Data Distribution lesson, Document 625-CD-009-002)].

7 On the DDIST host (e.g., **e0dis02**, **g0dis02**, **l0dis02**, **n0dis02**), examine the log **EcDsDistributionServerDebug.log** to determine if an e-mail notification was sent to the user identified in the subscription; the output should be similar to the following:

```
05/06/99 12:52:41: Media::SendNotificationMessage.(myNotify,mySite,myConfig-
>GetMode(),mailAddress): (, , TS1, cmts1@t1ins02u.ecs.nasa.gov
Media::SendNotificationMessage: Getting e-mail address from configuration file.
05/06/99 12:52:41: DdDsDoneQueue::Thread Was marked SyncDone and Signaled.
RequestID= 125125210220554
```

- The timing of this step may depend on the type of distribution being requested. If it is an FTPpull, the e-mail notification of data availability occurs prior to the pull attempt. If it is an FTPpush or a media distribution, the e-mail notification occurs after the data are shipped.

8 Examine the server logs to determine where the order failed, using the procedure for **Checking Server Log Files (Procedure 2.2)** (previous section of this lesson). Check **EcDmV0ToECSGatewayDebug.log** on the V0GTWY host (e.g., **e0ins02**, **g0ins02**, **l0ins02**, **n0ins02**), **EcDsStFtpDisServerDebug.log**, **EcDsStArchiveServerDebug.log**, **EcDsStStagingDiskServerDebug.log**, and **EcDsStStagingMonitorServerDebug.log** on the STMGT host (e.g., **e0drg01**, **g0drg01**, **l0drg01**, **n0drg01**), **EcDsScienceDataServerDebug.log** on the SDSRV host (e.g., **e0acs03**, **g0acs03**, **l0acs03**, **n0acs04**), and **EcDsDistributionServerDebug.log** on the DDIST host (e.g., **e0dis02**, **g0dis02**, **l0dis02**, **n0dis02**). Also check related .ALOG files.

- Look specifically at the SDSRV .ALOG (**EcDsScienceDataServer.ALOG**) for evidence that the request was received. You should see information similar to the following for FTPpull:

Priority: 0 Time : 05/18/99 10:44:55
PID : 5722:MsgLink :0 meaningfulname :DsSrSessionExecuteRequestStart0
Msg: Request ID 3c82feee-0d30-11d3-a305-c676e82eaa77:????: executing:
DsSrRequest (1): DsShSciRequestImp: [svr: ScienceDS, pri: NORMAL domain:0:]: (DsShSciCommandImp: service: ACQUIRE num parameters: 2 category: Parameters are:- UnnamedPL[DDISTMEDIATYPE(FtpPull) ECSUSERPROFILE(L7CPF-Pull)] DISTRIBUTION)

or the following for FTPpush (note that information about FTP user is included):

Priority: 0 Time : 05/18/99 10:48:10
PID : 5722:MsgLink :0 meaningfulname :DsSrSessionExecuteRequestStart0
Msg: Request ID b0f09aac-0d30-11d3-a305-c676e82eaa77:????: executing:
DsSrRequest (1): DsShSciRequestImp: [svr: ScienceDS, pri: NORMAL domain:0:]: (DsShSciCommandImp: service: ACQUIRE num parameters: 7 category: Parameters are:- UnnamedPL[DDISTMEDIATYPE(FtpPush) DDISTMEDIAFMT(FILEFORMAT) ECSUSERPROFILE(L7CPF-Push) FTPUSER(cmshared) FTPPASSWORD(********) FTPHOST(t1acs03) FTPPUSHDEST(/home/bmyer/TS1_data)] DISTRIBUTION)

- ***Note***: It is also possible to examine the System Requests displayed on the Science Data Server GUI to determine if SDSRV received the acquire request from the V0GTWY [use procedure **Monitor Science Data Server Request Processing** (Document 611-CD-510-001, Section 16.7.5)].

- If appropriate entries are missing, or there is other evidence of a communications disruption or failure, perform the procedure **Recovering from a Connectivity/DCE Problem (Procedure 3.1)** (previous section of this lesson).

9 Determine if there are data in the staging area, performing any corrective actions necessary.

- Use Steps 4 - 9 of the procedure for **Handling an Acquire Failure (Procedure 8.1)** (previous section of this lesson).

10 Execute *cdsping* of machines with which DDIST communicates from ***x*0dis02** [refer to the procedure for **Using ECS Assistant to Monitor Server Status** (Document 611-CD-510-001, Section 3.7.3.2)].

- It may be necessary to reboot any machine(s) from which there is no response [refer to the procedure for **Warm - By Subsystem Startup** (Document 611-CD-510-001, Section 3.1.1.2)].

11 On the System Management Support Subsystem (MSS) host (e.g., **e0mss21**, **g0mss21**, **l0mss21**, **n0mss21**), launch the ECS Order Tracking GUI and determine if the order is reflected in MSS order tracking [refer to the procedure for **ECS Order Tracking** (Document 611-CD-510-001, Section 19.3.1)].

- If the ECS Order Tracking GUI does not reflect the order, it may be instructive to examine the Order Tracking database (Database Administrator function) by logging into Sybase on the relevant MSS host [use procedure similar to steps 4 and 5 of **Recovering from a Subscription Server Problem (Procedure 6.1)** (previous section of this lesson)] and then selecting the User Name.

- If the order is not reflected in the Order Tracking database, perform the procedure for **Recovery from a Database Access Problem (Procedure 4.1)** (previous section of this lesson).

12 If the order is for an L7 scene, on the DSS working storage host (e.g., **e0wkg01**, **g0wkg01**, **l0wkg01**) examine the HDFEOS Server log (**EcDsHdfEosServer.ALOG**) to ensure that the HDF Server received the request. The log should contain entries similar to the following:

```
PID : 728:MsgLink :0 meaningfulname :DsCsOutputFileOpenHDFEOSFileSuccess
 Msg: HDFEOS output file opened Priority: 0 Time : 05/17/99 15:41:20
PID : 728:MsgLink :0 meaningfulname
:DsHrDCENonConfConcreteNonConfGetAsyncResultsAsyncRPCDoneOk
 Msg: Asynchronous RPC has finished with status OK.
 Priority: 0 Time : 05/17/99 15:41:20
PID : 728:MsgLink :0 meaningfulname :DsCsOutputFileCloseOutputFileSuccessful
 Msg: HDFEOS output file closed Priority: 0 Time : 05/17/99 15:41:20
```

- If the log does not reflect the request, perform the procedure **Recovering from a Connectivity/DCE Problem (Procedure 3.1)** (previous section of this lesson).

Recovering from Data Distribution Problems

Data distribution is key to any ECS functions that require the copying of data from the Archive. These functions include not only providing data to external users, but also providing data to internal ECS components.

Distribution on various media (e.g., 8mm tape) is generally limited to providing data for external users. The FTPpull process is also generally for external distribution. It is needed to fulfill L7 data orders and other FTPpull orders. The FTPpush process is central to many key ECS functions. For example, it is the means by which data are distributed among components of ECS (e.g., as needed for data processing). Therefore, FTPpush must be working in order to run PGEs. All ECS data distributions are dependent on the presence of the required data in the SDSRV database and in the Archive.

The distribution process may be tested in an acquire with the DSS Driver. The FTP processes use the FtpDis server. The FTPpull process uses the FTPpull Monitor server. Media distributions use appropriate servers for peripheral media. Therefore, the appropriate servers must be up and functioning correctly in order for data distribution to be successful. Use the following procedure to recover from data distribution problems.

Recovering from Data Distribution Problems (Procedure 14.1)

1 Ensure that the Data Distribution personnel have attempted appropriate operational solutions.

- Refer to the section on Troubleshooting Data Distribution Problems and the procedure for **Recovering from a Data Distribution Failure** in the training lesson on Data Distribution (Document 625-CD-509-002).

2 Use the Data Distribution (DDIST) GUI to determine if DDIST is handling a request for the data and to monitor the progress of the request [refer to the procedure for **Monitoring/Controlling Data Distribution Requests (**Document 611-CD-510-001, Section 18.2.2)].

- The DDIST GUI can be used to monitor the distribution request that is the focus of the problem. For troubleshooting/test purposes, use the DSS Driver to execute an acquire by the relevant distribution method and monitor its progress. A DSS Driver acquire uses system resources similar to those involved in a distribution of data to end users, although the resources used for a DSS Driver FTPpush are somewhat different from the system resources used in an internal distribution (e.g., for processing).

3 On the destination host for the files, execute **ls -l** command(s) to determine if the directory exists.

- If the appropriate directory is reflected, go to Step 5.
- If the directory does not exist, it is necessary to create it (e.g., have Production Planning and Processing personnel ensure that the target directory exists, creating it if necessary, or use the command **mkdir <*directory name*>**).
- ***Note***: If the distribution is for FTPpush to a user outside of ECS, it may be necessary to coordinate with that user to ensure that you have the correct information about the path to which the data are to be pushed, or that the appropriate directory is available.

4 For an internal push or pull by FTP, examine the server logs to determine if the files were distributed to the correct directory, using the procedure for **Checking Server Log Files (Procedure 2.2)** (previous section of this lesson).

- If the server log **EcDsStFtpDisServerDebug.log** on the STMGT host (e.g., **e0drg01**, **g0drg01**, **l0drg01**, **n0drg01**) properly reflects the push in an entry similar to the following, go to Step 6:

Pushing /usr/ecs/<*mode*>/CUSTOM/drp/<*host*>/data/staging//user3/:SC:AST_L1B.001:1384:1.HDF-EOS to /usr/ecs/<*mode*>/CUSTOM/pdps/<*host*>/data//DpPrRm/<*host*>_disk/AST_L1B_DataGranule.

- ***Note***: For FTPpush to end users, the server log of interest is **EcDsStFtpDisServerDebug.log** on the APC Server (e.g., **e0acg01**, **g0acg01**, **l0acg02**, **n0acg01**), and the path to which the data are pushed should reflect a location external to ECS.

- If there is no entry, examine the DDIST log **EcDsDistributionServerDebug.log** on the DDIST host (e.g., **e0dis02**, **g0dis02**, **l0dis02**, **n0dis02**) for indication that the distribution has been suspended or that there is some other problem with the distribution; if necessary perform the procedure **Recovering from a Data Distribution Failure** (Data Distribution Lesson, Document 625-CD-509-002).

5 Examine the server log (**EcDsStFtpDisServerDebug.log**) for an attempt to write to the directory with the result "Permission Denied," using the procedure for **Checking Server Log Files (Procedure 2.2)** (previous section of this lesson).

- If there is no evidence of incorrect permissions, go to Step 6 to determine if there are data in the staging area for the push.

- Incorrect permissions can be corrected by using a different account with the correct permissions, or by resetting the permissions. For Production Planning and Processing functions, it may be necessary to set up specific accounts planned for use in those functions.

6 On the appropriate host (e.g., **e0drg01**, **g0drg01**, **l0drg01**, **n0drg01**), type **cd /usr/ecs/<*mode*>/CUSTOM/drp/<*host*>/data/staging/<user>** and then press the **Return/Enter** key.

- The prompt reflects the change to the specified directory.

7 Type **ls** and then press the **Return/Enter** key.

- If the file(s) are properly listed in output similar to the following, go to Step 8:

:SC:AST_L1BT.001:1411:1.HDF-EOS SCAST_L1BT.11411.met
Niger-L1B-4.hdf staging.disk.filename.list
PACKING.LST.582292669708

- If the file(s) are not listed, it may indicate that there is insufficient space in the staging area for the staging disk. Examine the DDIST log **EcDsDistributionServer Debug.log** on the DDIST host (e.g., **e0dis02**, **g0dis02**, **l0dis02**, **n0dis02**) for

indication of that or other problem with the distribution; if necessary perform the procedure **Recovering from a Data Distribution Failure** (Data Distribution Lesson, Document 625-CD-009-002).

8 Examine the server logs to determine the last successful communication, using the procedure for **Checking Server Log Files (Procedure 2.2)** (previous section of this lesson). Check **EcDsStFtpDisServerDebug.log**, **EcDsStArchiveServerDebug.log**, **EcDsStStagingDiskServerDebug.log**, and **EcDsStStagingMonitorServerDebug.log** on the STMGT host (e.g., **e0drg01**, **g0drg01**, **l0drg01**, **n0drg01**), **EcDsScienceData ServerDebug.log** on the SDSRV host (e.g., **e0acs03**, **g0acs03**, **l0acs03**, **n0acs04**), and **EcDsDistributionServerDebug.log** on the DDIST host (e.g., **e0dis02**, **g0dis02**, **l0dis02**, **n0dis02**).

- If there is evidence of a communications disruption or failure, perform the procedure **Recovering from a Connectivity/DCE Problem (Procedure 3.1)** (previous section of this lesson).

9 Execute *cdsping* of machines with which DDIST communicates from ***x*0dis02** [refer to the procedure for **Using ECS Assistant to Monitor Server Status** (Document 611-CD-510-001, Section 3.7.3.2)].

- It may be necessary to reboot any machine(s) from which there is no response [refer to the procedure for **Warm - By Subsystem Startup** (Document 611-CD-510-001, Section 3.1.1.2)].

Recovering from Problems with Submission of an ASTER Data Acquisition Request (EDC Only)

Authorized scientists will use the ECS Java DAR Tool to submit ASTER Data Acquisition Requests to the ASTER Ground Data System (GDS) in Japan. The Java DAR Tool and submission of DARs is supported by the EROS Data Center (EDC), where associated subscriptions are placed for notification that the data resulting from the requests have been received, and where the data will be archived. Use the following procedure to recover from problems with submission of an ASTER DAR.

Recovering from Problems with Submission of an ASTER Data Acquisition Request

1 Check to ensure that the user attempting the DAR submission is an ECS User with a registered account with DAR permissions enabled.

- Use the ECS Account Management GUI to profile the user's account and review the associated DAR Information [refer to **Edit/Modify DAR Information** (Document 611-CD-510-001, section 19.1.4.6)]. If the user is not authorized to submit a DAR, it

may be necessary to refer that user to the U.S. ASTER website at **http://asterweb.jpl.nasa.gov**.

- (**Note**: When a user account is authorized for DAR permissions, ECS submits a request to the ASTER GDS for establishment of a corresponding authorization there. If an otherwise authorized user receives a message on the Java DAR Tool refusing a DAR submission, it may be necessary to coordinate with the ASTER GDS to verify that they have taken the action necessary to establish an account there.)

2 Verify that the necessary servers are "up" and listening; use the command line **ps -ef | grep <*server process*>**, or monitor server status using ECS Assistant or HP OpenView [refer to **Using ECS Assistant to Monitor Server Status** and **cdsping all servers** (Document 611-CD-510-001, section 3.7.3.2) or **Using HP OpenView to Check the Status of Hosts and Servers** (previous section of this lesson), and, if necessary, **Start an Application/Program** (Document 611-CD-510-001, section 7.3.2)]. The following servers are necessary:

- EcMsAcRegUserSrvr (on e0mss21).
- EcGwDARServer (on e0ins01).
- EcSbSubSrvr (on e0ins01).
- EcCsMojoGateway (on e0ins01).
- EcClWbJessProxyServer (on e0ins02).
- EcClWbFoliodProxyServer (on e0ins02).
- EcIoAdServer (on e0ins02).

3 Check the DAR Gateway configuration file (EcGwDARServer.CFG) to make sure that it reflects the correct IP address and port number for the ASTER GDS.

- Use the UNIX **view**, **pg**, or **vi** command to view the contents of the file. Near the end of the file, you should see an entry similar to the following:

```
#GDS API parameters
GdsIPAddress        = 210.138.101.43
GdsPort             = 10500
GdsTimeOut          = 10
```

(**Note**: The specific IP Address and Port should be set to values that are correct for the ASTER GDS. During testing before operational connection to the GDS, these values are set to reflect site-specific and mode-specific connection to the ASTER GDS simulator.)

4 Examine the server log files for activity reflecting the DAR submission [refer to the procedure for **Checking Server Log Files (Procedure 2.2)** (previous section of this lesson)].

- The **EcClWbJessProxyServerDebug.log** should reflect use of the Java DAR Tool to create a DAR with entries similar to the following:

```
Using /usr/ecs/TS1/CUSTOM/jdt/htdocs/conf/jdt.cfg to access properties
Using /usr/ecs/TS1/CUSTOM/jdt/htdocs/conf/gui.cfg to access properties
Servlet.AttributeServlet(942338905240):initialized
{Root, Root, 942338909056, 499530658}
    {Untitled Folder, Folder, 4242424242424242, 499531739}
        {0, XAR, 942338925546, 499529412}
            {General - Primary Attributes, PrimaryAttribute, 942338925608, 499524693}
            {General - Telescope Gains, TelescopeSetting, 942338925643, 499533322}
            {Spatial, SpatialSetting, 942338925724, 499533250}
            {Temporal, TemporalSetting, 942338925911, 499530170}
            {Coverage, CoverageDetailsSetting, 942338925991, 499529226}
.
.
.
```

and then indicate successful communication with the ASTER Ground Data System to submit the DAR and receive a DAR ID.

- If the logs do not reflect appropriate activity associated with the submission of the DAR, ensure that the involved servers are up and listening [refer to **Using HP OpenView to Check the Status of Hosts and Servers** (previous section of this lesson), and, if necessary, **Start an Application/Program** (Document 611-CD-510-001, Section 7.3.2)]. It may also be necessary to ensure that DCE is functioning properly [refer to the procedure for **Recovering from a DCE/Connectivity Problem (Procedure 3.1)** (previous section of this lesson)].

  Error indications in the **EcClWbJessProxyServerDebug.log** may be similar to the following:

```
10/25/99 15:14:00: handleSIGCHLD was invoked!
JESS terminated for some reason
Please review the JESS logs for details!
10/25/99 15:14:00: Inside PfShutdown()
10/25/99 15:14:00: Leaving PfShutdown!
10/25/99 15:14:00: Called EcClWbJessProxyServer::DCEServerShutdown()
10/25/99 15:14:00: bStopRecoveryThread == EcDTrue ---> goto DoneProcessingEvents
10/25/99 15:14:00: Leaving the EcAgManager desctructor
15:14:01.2700 001 Client-22977 Error: exception caught in ~DCEServer:
15:14:01.2809 001 Client-22977 Not registered in endpoint map (dce / rpc)
```

and:

JDT::Error[999]:FATAL:jdt.services.xar.SubmissionAgent:REQUEST_HANDLING:ClWbJt.mojo.ConnectionException: ErrorCode 15011
Error received from GDS

ClWbJt.mojo.ConnectionException: ErrorCode 15011
.
.
.

5 Check the Subscription Server GUI to ensure that a subscription is registered for the DAR [refer to the procedure for **Returning a List of Subscriptions** (Document 611-CD-510-001, Section 19.4.3)].

- If the subscription is not reflected on the Subscription Server GUI, use the procedure **Checking Server Log Files** (previous section of this lesson) to determine if the **EcCsMojoGatewayDebug.log** indicates that a subscription request was sent to the subscription server, and to determine if the **EcSbSubServerDebug.log** indicates that the subscription server received the subscription request.
- If the subscription was not registered, check that the Subscription function is working properly [refer to the procedure for **Recovering from a Subscription Server Problem (Procedure 6.1)** (previous section of this lesson)].

This page intentionally left blank.

Trouble Ticket (TT)

We have seen that a system problem is typically documented using the Remedy COTS software product to prepare and update a problem report or trouble ticket (TT). Because there is a separate lesson that covers writing a trouble ticket, documenting changes, preparing and processing a trouble ticket through the failure resolution process, and making emergency fixes, these topics are not addressed in detail here. By now you are familiar with the requirements for using trouble tickets in ECS problem management. You know that troubleshooting and repair activities that involve changes to the system configuration require a configuration change request (CCR).

Using Problem Report Software

Although you are familiar with using Remedy to create and view trouble tickets, there are other functions associated with the maintenance and operation of the trouble ticket service that you may be required to manage as a System Administrator or other manager. Specifically, the following tasks associated with Remedy may be required of the TT administrator or others:

- adding users to Remedy.
- controlling and changing privileges in Remedy.
- modifying Remedy's configuration.
- generating Trouble Ticket reports.

Let's look at each of these functions.

Adding Users to Remedy

The TT Administrator uses the Remedy User schema to grant access to the Remedy tool. Users who leave the ECS program can be deleted. The Remedy *Action Request System Administrator's Guide*, Chapter 2, "Defining Access Control," summarizes license elements and access control. There are no license restrictions on the number of users who can be granted permission to create and query trouble tickets. The chapter also provides instructions on using the **User** schema (a "schema" represents a table in the Remedy database) to add registered users.

Figure 22 shows the screen layout for the Remedy **User** schema that is used for adding users. This screen is accessible to administrators with Administrator Group privileges by entering a Unix command beginning with the directory where Remedy is installed and invoking the user tool (e.g., on **l0msh03**, enter command **/usr/ecs/*mode*/COTS/remedy/bin/aruser &**). This results in display of the user tool, from which you launch the **User** schema.

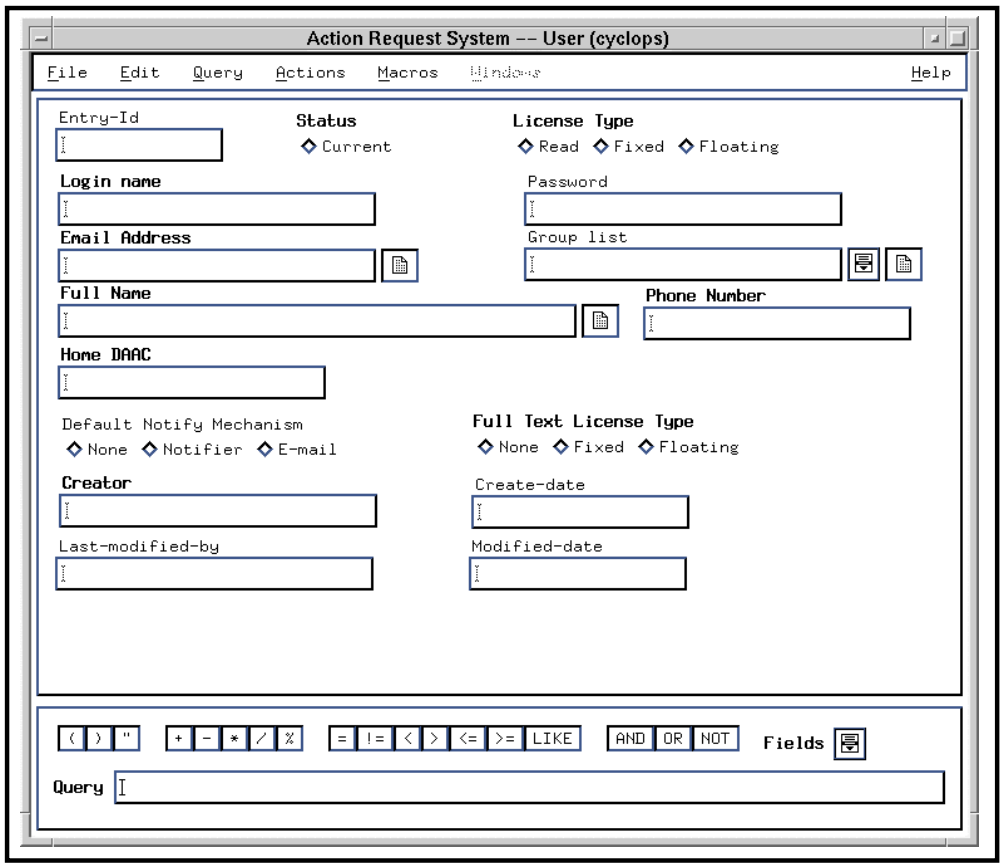


Figure 22. Remedy User Schema

Suppose, for example, that you wish to add Terry Bulticketer from the GSFC DAAC as a user with submit and query permissions. His e-mail address is tbultick@ecsgsfc1.gsfc.nasa.gov, and his phone number is 301-614-4132. The data to be entered to add a user include:

- Status – is the user current or not?
- License Type – what type of license does the user have? The default, **Read**, includes submit and query permission.
- Login Name – the identifying name the user will enter to use the Remedy tool.
- Password – the identifying password the user will enter to use the Remedy tool.
- Email Address – the e-mail address of the user.
- Group List – specifies a user's access control groups; must be left empty to grant only basic submit and query privileges.
- Full Name – the user's full name.
- Phone Number – the user's telephone number.
- Home DAAC – the user's home DAAC.

- Default Notify Mechanism – the way in which the user will be notified of actions; if left blank, the method can be specified at the time an action is taken.
- Full Text License – the type of full text search license the user is to have; the default is **None**, which is what users will be assigned (full-text search is not part of ECS).
- Creator – the person who created the account.

The system generates the content of the other fields. Use the following procedure.

Adding a User to Remedy

1 Follow menu path **File→Open Schema**.

- The **Open Schema** dialog box is displayed.

2 Double click on **User** from the list in the Open Schema dialog box, or click on **User** to highlight it and then click on the **Apply** button to load the schema.

3 Follow menu path **File→Open Submit**.

- A **Submit** window is displayed.

4 If necessary, click on the toggle button in front of **Current** to indicate the user's status (**Current** is the default).

5 Click on the toggle button in front of the desired license type (in this case, **Read**).

6 Enter the login name (in this case, **tbultick**) to be used to access Remedy into the **Login Name** field.

7 Enter the user's e-mail address (in this case, **tbultick@ecsgsfc1.gsfc.nasa.gov**) in the **Email Address** field.

8 Enter the user's full name (**Terry Bulticketer**) in the **Full Name** field.

9 Enter the user's telephone number (**301-614-4132**) in the **Phone Number** field.

10 Enter the user's home DAAC (**GSFC**) in the **Home DAAC** field.

11 If you wish to select a default notification mechanism (e.g., e-mail), click on the toggle button in front of the desired selection (in this case, **E-mail**).

12 For **Full Text License Type**, ensure that the default, **None**, is selected; if necessary click on the toggle button in front of **None**.

13 Enter your name in the **Creator** field.

14 Click on the **Apply** button.

- The information is saved to the database.

15 Click on the **Dismiss** button.

Changing Privileges in Remedy

Changing privileges in Remedy, or controlling privileges of those who have access to Remedy, is done by the TT Administrator. There are 18 Remedy privilege groups for ECS, and a change to the privileges of any group requires an approved Configuration Change Request (CCR). Access privileges provide permission to view a field, or to change it. The groups and their access privileges are defined in Document 611-CD-510-001 *Mission Operation Procedures for the ECS Project*, Section 8.2.6.

The Remedy *Administrator's Guide for OSF/Motif*, Chapter 3, "Setting Up Users and Groups," provides detailed information about access control and privileges. The administrator defines groups of users by using the User Tool to change the Group schema. A user's privileges may be changed in two ways:

- changing the group to which the user is assigned.
- changing the access privileges of the group.

We have seen that the **User** schema is used to implement group assignment. To change the access privileges of a group, you use the **Admin** tool. It is accessed by entering a Unix command beginning with the directory where Remedy is installed and invoking the tool with an option (e.g., **<*ar_install_dir*>/bin/aradmin -s &**). Use of the option **-s** results in display of the Admin tool with the **Schemas** list displayed, as illustrated in Figure 23.

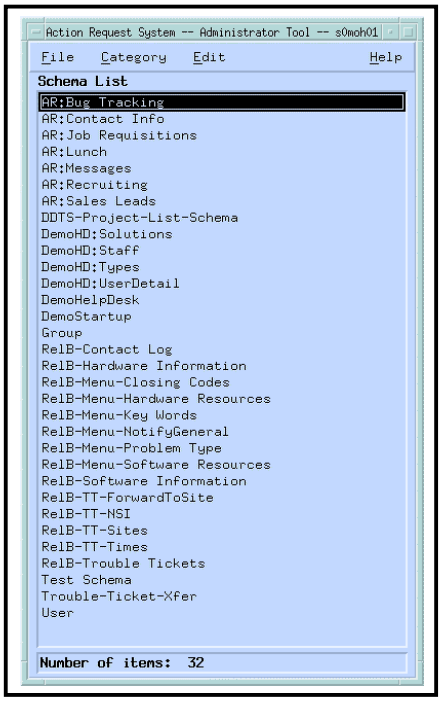


Figure 23. Remedy Admin Tool, Schema List

You set the schemas accessible to a group by selecting schema permissions in the **Group Access** window, illustrated in Figure 24.

Figure 24. Remedy Admin, Group Access Window

Use the following procedure to define group access for schemas (Remedy database tables)

Defining Group Access for Schemas

1 Follow menu path **Edit→Group Access**.

- The **Group Access** window is displayed

2 Click on the **Group** list menu symbol icon (located at the right side of the **Group** field).

- The **Groups** selection menu is displayed.

3 Select a group from the selection menu.

- The Group Access window indicates current permission settings for the selected group by means of radio buttons for each schema in the list, showing:
  - *visible* (i.e., available in the list of **Schemas** that can be opened by users in the selected group).
  - *hidden* (i.e., not available in the list of **Schemas** that can be opened by users in the selected group, except that users who have **Customize** permissions can make a hidden field visible).
  - *none* (i.e., not available).

4 For each item, set the schema permissions for the specified group, clicking on the appropriate radio button to select **visible**, **hidden**, or **none** as the permission for each schema.

5 Click on the **Apply** button.

- The option settings are saved.

6 Click on the **Dismiss** button.

- The window is closed.

The **Group Access – Schema Fields** window allows you to determine **View** or **Change** access to field data. It is accessible from the **Modify Schema** window, shown in Figure 25. The following procedure is applicable.

Defining Group Access for Schema Fields

1 From the **Schema List** in the **Admin Tool**, open a schema by double clicking on it.

- The **Modify Schema** window is displayed.

2 Follow menu path **Attributes→Field Group Access**.

- The **Group Access – Schema Fields** window is displayed.

3 Click on the **Group** list menu symbol icon.

- The **Groups** selection menu is displayed.

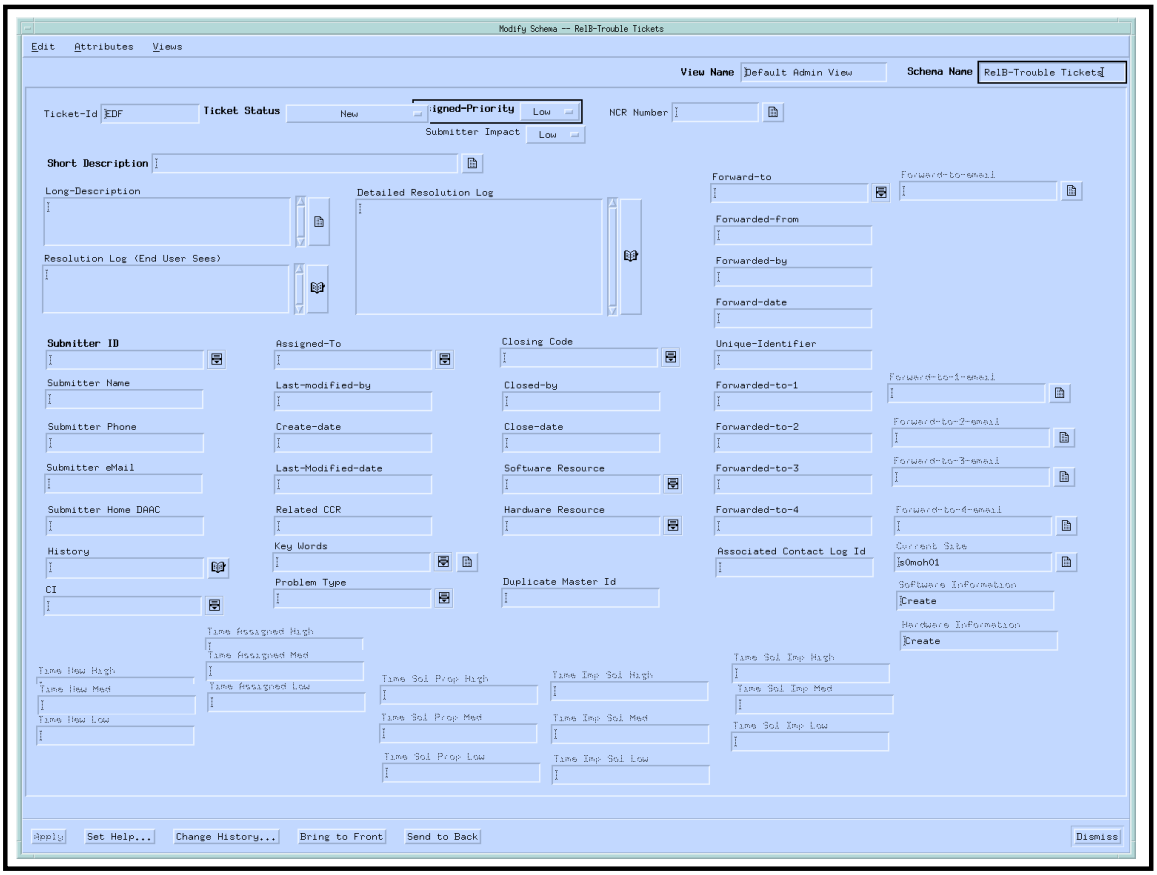


Figure 25. Remedy Admin - Modify Schema

4 Select a group from the selection menu.

- The **Group Access – Schema Fields** window displays buttons that differ according to the group chosen.
- Groups with a group type of **View** only allow you to select View permissions for schema fields.
- Groups with a group type of **Change** allow you to select View and Change permissions.

5 Set the permissions for each field.

- Selecting **View** allows users to view the field data in the schema. Selecting **Change** allows users to view and change the field data in the schema.

6 Click on the **Apply** button.

- The permission settings are saved.

7 Click on the **Dismiss** button.

- The Group Access - Schema Fields window is closed.

8 Click on the **Apply** button in the Modify Schema window.

- The changes are now applied to the schema.

9 Click on the Click on the **Group** list menu symbol icon.

- The **Groups** selection menu is displayed.

10 Click on the **Dismiss** button.

- The **Modify Schema** window is closed.

Changing Remedy Configuration

The RelB-Trouble Tickets schema, or Trouble Ticket screen, contains several fields that provide picklists, or pull-down lists of valid entries from which a user can select in filling out a trouble ticket. During ECS deployment, it may be necessary or desirable to change the items in some of these picklists. Fields that provide picklists that may be modified are:

- User Contact Log (CL) Category.
- User Contact Log (CL) Contact Method.
- Configuration Item (CI).

Administrators with appropriate access can customize the pull-down pick-lists in a Remedy schema. This is accomplished through the Admin Tool by modifying the **RelB-CI**, **RelB-CL-Category**, and **RelB-CL-Contact Method** schemas, using the **Modify Menu** window illustrated in Figure 26. Procedure 8.2.7 in Document 611-CD-510-001 *Mission Operation Procedures for the ECS Project* refers to appropriate sections in the Remedy User's Guide and the Remedy Administrator's Guide. An approved Configuration Change Request (CCR) is required before implementing any of these changes.

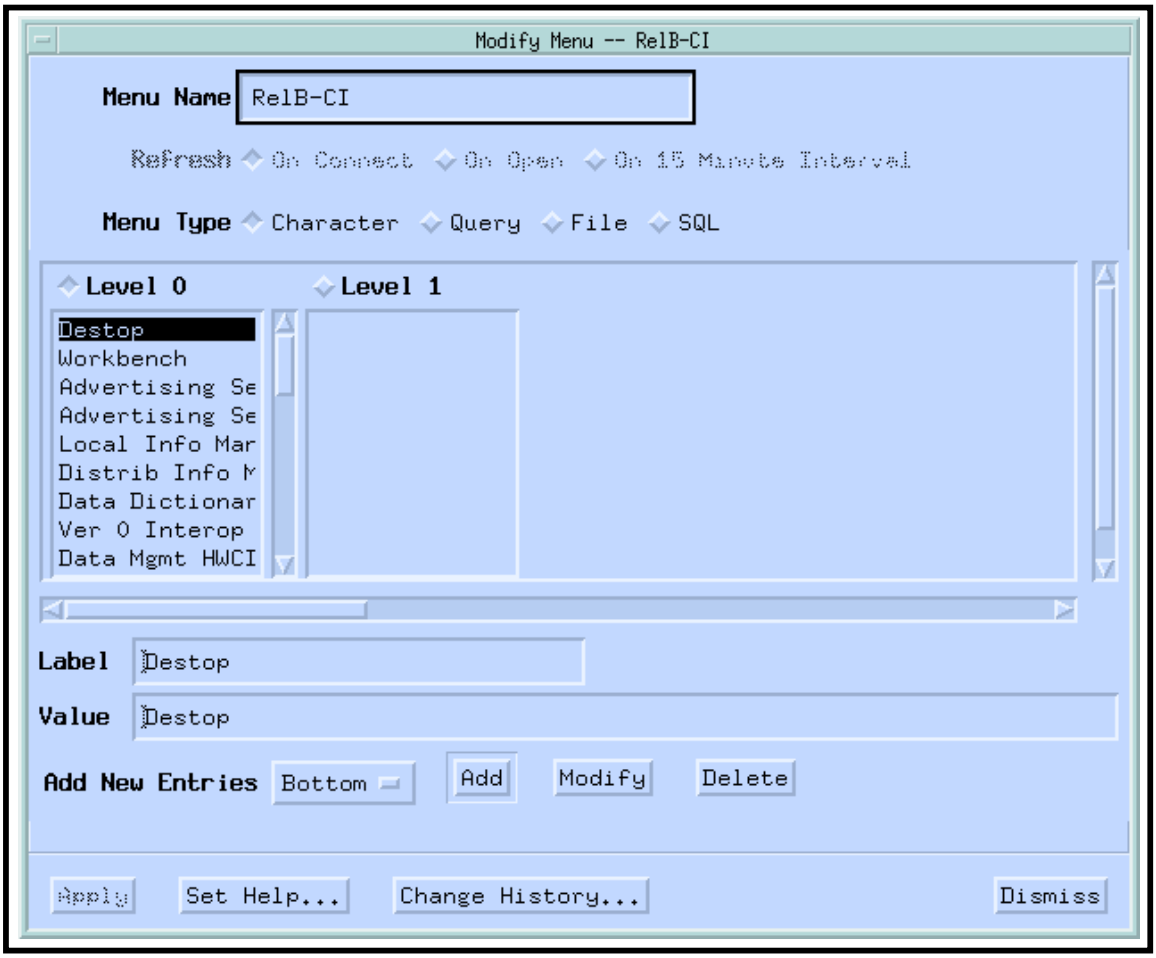


Figure 26. Remedy Modify Menu Window

Modifying Remedy's Configuration uses the following procedure.

Modifying Remedy's Configuration

1 Follow the **Category→Menus** menu path of the Admin Tool main window

- The **Menu List** is displayed in the **Admin Tool**.

2 From the **Menu List** in the **Admin Tool**, open a menu by double-clicking on it.

- Select from the list one of the following: **RelB-CI**, **RelB-CL-Category**, and **RelB-CL-Contact Method**.
- The **Modify Menu** window is displayed.

3 Select the level for which you want to add or modify menu choices by selecting the radio button next to the level's label.

- To add or modify menu choices at the highest level, select Level 0. Select each successive menu level to modify the choices at that level.
- Menu choices added at levels below the top level (level 0) will be sub-items of the selected item at the next highest menu level.

4 Enter a label (the text that will show up in the menu).

- Enter a maximum of 30 characters.

5 If the text that you want to appear when the user selects this menu item differs from the label text, enter the text you want to appear in the Value field.

- Enter a maximum of 255 characters.
- If you do not enter different text, the label text (of the lowest menu level only) will be displayed when the user selects the item.

6 From the Add New Entries selection menu, select an option to determine whether the entry you are defining is added to the top of the current list of selections, the bottom of the list, or before or after the item that is currently selected.

7 Select **Apply** to add the item to the list, or select **Modify** to replace the currently selected item with the new label and text.

8 Repeat steps 3 through 7 for as many items as are needed at that menu level.

Generating Trouble Ticket Reports

A set of predefined reports is maintained in a public directory that should be downloaded to your personal configuration directory. Procedure 8.2.8 in Document 611-CD-510-001 *Mission Operation Procedures for the ECS Project* refers to appropriate instructions in the Remedy User's Guide for copying files to share macros and custom reports. These reports are trouble ticket administrative reports generated for local and system-wide usage. There are several types of predefined reports, including:

- Assigned-to Report – provides a report of the number of Tickets assigned to technicians.
- Average Time to Close TTs – provides a report of the average time to close trouble tickets.
- Hardware Resource Report – provides a report sorted and grouped by Hardware Resources and Closing Codes.

- Number of Tickets by Status – provides the number of Trouble Tickets grouped by Status.
- Number of Tickets by Priority – provides the number of Trouble Tickets grouped by assigned priority.
- Review Board Report – provides a report of the details of TTs for the TT Review Board.
- SMC TT Report – provides a report to be sent to the SMC.
- Software Resource Report – provides a report sorted by Software Resources and their Closing Codes.
- Submitter Report – indicates by submitter the number and type of trouble tickets in the system.
- Ticket Status Report – provides a report sorted and grouped by Ticket Status.
- Ticket Status by Assigned-to – provides a report sorted and grouped by the last person assigned to a Trouble Ticket.

Procedure 8.2.8 in Document 611-CD-510-001 *Mission Operation Procedures for the ECS Project* refers to the Remedy User's Guide, Chapter 5, "Reports" for instructions on working with reports. Most of the time, you will probably select a report from the list, using the **Report** window illustrated in Figure 27. If you choose to create your own custom report, these instructions provide detailed guidance on selecting report content, setting report layout, specifying the sorting and grouping of report content, generating statistics, setting report options, saving, using, and modifying custom reports, and generating report output.

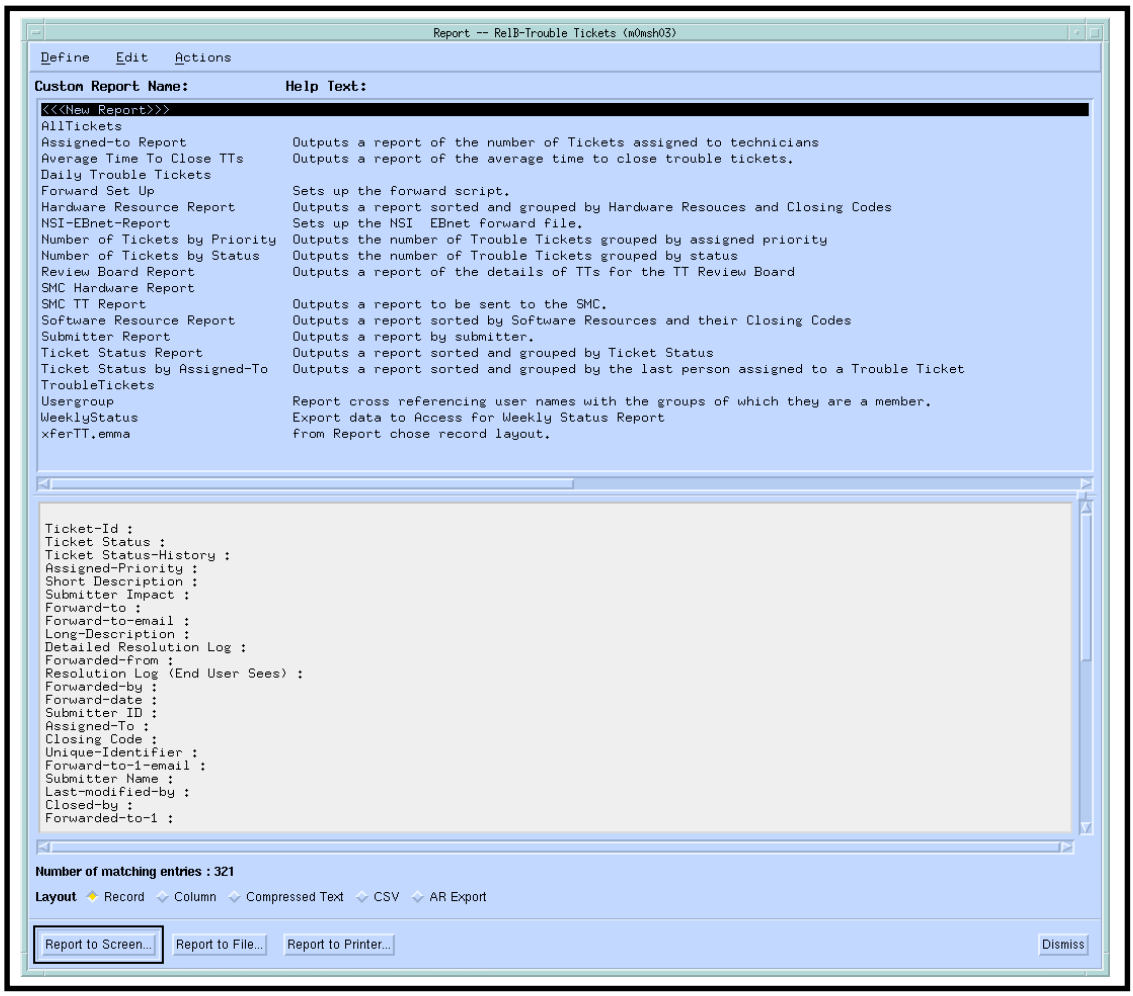


Figure 27. Remedy Report Window

Suppose you want to print a report on one of the provided custom reports, Ticket Status Report. Use the following procedure to create and print the report.

Using a Custom Report

1 Select the schema you want to work with by selecting the schema name in the Available Schemas list and then selecting the **Apply** button, or by double-clicking on the schema name (in this case, **RelB-Trouble Tickets**).

2 Define the query criteria to be applied to the search by filling in fields in the **Query** window or by using the query bar. (In this case, request all trouble tickets by clearing all fields and leaving the **Query** window blank.)

- The query will return all RelB-Trouble Tickets.

3 From the Trouble Ticket main window in the User Tool, follow menu path **Query→Report**.

- The **Report** dialog box appears.

4 Select the report you want from the **Custom Report Name** list by clicking on the report name (in this case, **Ticket Status Report**).

- The **Custom Report Name** list contains all custom report files that are in all directories defined in your Path preference.
- The custom report **Ticket Status Report** is loaded into the Report window with the report prototype visible. The custom report layout and page setup are applied to the set of trouble tickets defined in the query criteria.

5 Click on the **Report to Printer** button in the **Report** window.

- If you have specified the print setup for the report, the report is printed. If you have not yet specified the print setup, the **Report Print - <*schema*>** dialog box appears.
  a) Specify whether you want to use the default printer or a specific printer by selecting from the list.
  b) Select the desired **Number of Copies**.
  c) Select the **Print** button to send your report to the printer.

Performing Operational Work-around

An operational work-around is a temporary modification to operations and user procedures that is entailed by resolution of a trouble ticket. It is characterized by several factors that may affect the way in which procedures are accomplished to conduct operations during the period of temporary inability to conduct operations using normal procedures:

- managed by the ECS Operations Coordinator at each center.
- master list of work-arounds and associated trouble tickets and configuration change requests (CCRs) kept in either hard-copy or soft-copy form for the operations staff.
- hard-copy and soft-copy procedure documents are “red-lined” for use by the operations staff.
- work-arounds affecting multiple sites are coordinated by the ECS organizations and monitored by ECS M&O Office staff.

The work-around is removed when the CCR that corrects the original problem is installed into the operational baseline.

Practical Exercise

Introduction

This exercise is designed to practice key elements of the System Troubleshooting procedures. Perform the tasks identified in the exercise.

Equipment and Materials

One ECS workstation, a copy of 625-CD-517-002 *ECS Training Material Volume 17: System Troubleshooting*, a copy of 609-CD-510-002 *Release 5B Operations Tools Manual*, and a copy of 611-CD-510-001 *Mission Operations Procedures for the ECS Project*.

Perform Activities Related to System Monitoring and Troubleshooting

1. Use ECS tools to perform system monitoring activities, including HP OpenView maps and event log files for checking the health and status of the network and the web browser to access the EBnet Web Page.
2. Use HP OpenView to check for event notifications, and browse the event logs for several event categories as you would to diagnose a problem event.
3. Use HP OpenView to view the status of servers in a subsystem (e.g., Data Server Subsystem). Use HP OpenView to view the status of all servers in the OPS mode; use HP OpenView to view the status of all servers in the TS1 mode.
4. Use the *cdsbrowser* to check DCE entries for servers.
5. Locate and review Debug.log and .ALOG files for SDSRV, ADSRV, SBSRV, DDICT, V0GTWY, INGST, Archive Server, STMGT, and PLANG.
6. Check mount points for PDPS on hosts for SDSRV and Archive Server.
7. Launch the SDSRV GUI and review the ESDTs listed on the Data Types tab.
8. Check the SDSRV cfg directory for *.evt files.
9. Launch the Data Dictionary Maintenance Tool and update the mapping for all collections.
10. List the contents of the Archive directory.
11. On host *x*0drg01, check the drp-mounted staging disk.
12. Add a user to Remedy. Then change that user's privileges in two ways: first, change the group to which the user is assigned; then, change the access privileges of the group to which you last assign the user.
13. Follow Procedure 8.2.7 in Document 611-CD-510-001 *Mission Operation Procedures for the ECS Project* and use the Remedy Admin Tool to add a key word to the **User Contact Log (CL) Contact Method** pull-down pick-list in the RelB-Trouble Ticket schema.

This page intentionally left blank.

Slide Presentation

Slide Presentation Description

The following slide presentation represents the slides used by the instructor during the conduct of this lesson.

This page intentionally left blank.